JURNAL VOKASI KESEHATAN

Tinjauan Keamanan Data Rekam Medis Elektronik Di Puskesmas Jabung

Review of Electronic Medical Record Data Security at Puskesmas Jabung

Lintang Dwi Maia Prabawati[1*], Fita Rusdian Ikawati [2], Lilik Afifah[3]
[1,2,3] Program Studi D-3 Rekam Medis dan Informasi Kesehatan, Institut Teknologi Sains dan Kesehatan Rs dr. Soepraoen Malang
***Corresponding Author:** lintangdwimp13@gmail.com

Sejarah artikel:
Diterima: 20 Mei 2025
Revisi: 10 Juni 2025
Diterima: 24 Juni 2025

Kata kunci:

Keamanan Data, Kerahasiaan, Integritas, Ketersediaan

ABSTRAK

Keamanan data dalam rekam medis elektronik (RME) merupakan aspek penting dalam perlindungan informasi di fasilitas pelayanan kesehatan. Puskesmas Jabung telah menerapkan sistem RME, namun masih terdapat kelemahan, seperti belum adanya fitur log out otomatis yang berpotensi meningkatkan risiko akses tidak sah. Penelitian ini bertujuan untuk meninjau keamanan data di Puskesmas Jabung berdasarkan aspek kerahasiaan, integritas, dan ketersediaan. Metode penelitian yang digunakan adalah kualitatif dengan pendekatan studi kasus. Data dikumpulkan melalui wawancara mendalam dan observasi terhadap kebijakan serta praktik keamanan yang diterapkan. Hasil penelitian menunjukkan bahwa dalam aspek kerahasiaan, sistem telah menerapkan pembatasan akses perpoli seperti username dan password pada saat log in, tetapi belum memiliki fitur log out otomatis. Pada aspek integritas, data telah dikatakan aman karena pengeditan hanya dapat dilakukan oleh pengguna yang berwenang sesuai hak akses, serta telah dilengkapi adanya audit log untuk mencatat perubahan data. Dalam aspek ketersediaan, sistem telah menggunakan backup otomatis ke cloud untuk menjaga keberlanjutan akses data, sehingga data tetap tersedia saat dibutuhkan. Optimalisasi sistem keamanan diperlukan untuk meningkatkan perlindungan data yang lebih baik.

Keywords:

Data Security, Confidentiality, Integrity, Availability.

ABSTRACT

Data security in electronic medical records (EMR) is a crucial aspect of information protection in healthcare facilities. Puskesmas Jabung has implemented an EMR system; however, certain security weaknesses remain, such as the absence of an automatic logout feature, which could increase the risk of unauthorized access. This study aims to review data security at Puskesmas Jabung based on the aspects of confidentiality, integrity, and availability. The research method used is qualitative with a case study approach. Data were collected through in-depth interviews and observations of security policies and practices. The findings indicate that in terms of confidentiality, the system has implemented access restrictions per polyclinic using usernames and passwords during login, but it lacks an automatic logout feature. Regarding integrity, data is considered secure as modifications can only be made by authorized users based on their access rights, and the system is equipped with an audit log to record data changes. In terms of availability, the system employs automatic cloud backups to ensure continuous access to data, making it readily available when

needed. Optimizing the security system is essential to enhance data protection and improve overall efficiency.

PENDAHULUAN

Rekam Medis Elektronik adalah Rekam Medis yang dibuat dengan menggunakan sistem elektronik yang diperuntukkan bagi penyelenggaraan Rekam Medis. Tujuan utama dari rekam medis elektronik adalah untuk peningkatan dalam penyimpanan, pemrosesan, dan pertukaran informasi kesehatan, yang pada akhirnya dapat meningkatkan kualitas pelayanan kesehatan secara keseluruhan, serta untuk memenuhi prinsip-prinsip keamanan dan kerahasiaan data informasi medis pasien, sehingga data dan informasi yang ada dalam Rekam Medis Elektronik terlindungi penggunaan dan penyebarannya (Widiyanti et al., 2024).

Keamanan data rekam medis elektronik merupakan aspek penting dalam perlindungan informasi pasien di fasilitas pelayanan kesehatan. Dalam rangka keamanan dan perlindungan data Rekam Medis Elektronik, pimpinan Fasilitas Pelayanan Kesehatan memberikan hak akses kepada Tenaga Kesehatan atau tenaga lain di Fasilitas Pelayanan Kesehatan, pemberian hak akses menjadi bagian dari kebijakan standar prosedur operasional penyelenggaraan Rekam Medis Elektronik yang ditetapkan oleh pimpinan Fasilitas Pelayanan Kesehatan, hak akses yang dimaksud terdiri atas hak untuk penginputan data, perbaikan data, dan melihat data. Pemerintah Indonesia telah mengatur standar keamanan data dalam Peraturan Menteri Kesehatan No. 24 Tahun 2022, yang menetapkan prinsip kerahasiaan, integritas, dan ketersediaan sebagai dasar perlindungan data dalam sistem RME.

Puskesmas Jabung Malang telah menerapkan sistem RME. Namun, Dalam penerapan di lapangan, masih ditemukan kelemahan dalam menjaga keamanan data, seperti pada kasus di Puskesmas Jabung. Berdasarkan hasil studi pendahuluan yang di lakukan pada tanggal 20 Mei 2024 hingga 14 Juni 2024, ditemukan bahwa di tempat pendaftaran pasien, akun pada aplikasi E-Pus beberapa kali tidak di log out sebelum komputer dimatikan. Akibatnya, saat komputer dinyalakan kembali, akses ke dalam data rekam medis langsung terbuka tanpa memerlukan log in ulang yang dapat berpotensi mengancam keamanan data pasien, beresiko disalahgunakan oleh pihak yang tidak bertanggung jawab (Suhariyono et al., 2025). Untuk meningkatkan keamanan data di Puskesmas Jabung diperlukan adanya fitur log out otomatis setelah penggunaan aplikasi dan pelatihan bagi tenaga Kesehatan mengenai pentingnya menjaga keamanan data dalam penggunaan sistem elektronik. Keamanan dan kerahasiaan informasi medis pasien menjadi salah satu hal penting yang perlu dipertimbangkan sesuai peraturan yang berlaku (Prisusanti & Afifah, 2022).

Penelitian ini bertujuan untuk meninjau keamanan data Rekam Medis Elektronik di Puskesmas Jabung berdasarkan aspek kerahasiaan, integritas, dan ketersediaan. Hasil dari penelitian ini diharapkan dapat memberikan wawasan serta rekomendasi untuk meningkatkan keamanan sistem, seperti penerapan fitur logout otomatis dan peningkatan kesadaran tenaga kesehatan terhadap praktik keamanan data dalam penggunaan sistem Rekam Medis Elektronik.

METODE

Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kasus karena memungkinkan eksplorasi mendalam terhadap fenomena yang terjadi secara nyata di lokasi penelitian, khususnya dalam aspek kerahasiaan, integritas, dan ketersediaan. Pelaksanaan berlangsung selama dua bulan, dari November hingga Desember 2024. Informan dalam penelitian ini dipilih menggunakan teknik purposive sampling, dengan mempertimbangkan peran mereka dalam pengelolaan sistem RME. Informan terdiri dari Kepala Instalasi Rekam Medis sebagai Informan Kunci, Petugas IT sebagai Informan Utama, serta Staf Rekam Medis pendaftaran, Dokter dan Perawat sebagai informan tambahan. Pemilihan informan didasarkan pada pengalaman mereka dalam menggunakan sistem RME, dengan kriteria tenaga kesehatan yang telah menggunakan aplikasi E-Puskesmas minimal 1 tahun untuk memastikan pemahaman yang cukup mengenai sistem keamanan data yang diterapkan.

Data yang digunakan dalam penelitian ini terdiri dari data primer dan data sekunder. Data primer diperoleh melalui wawancara mendalam dan observasi langsung terhadap praktik keamanan data dalam sistem RME di Puskesmas Jabung. Sementara itu, data sekunder berasal dari dokumen resmi, peraturan pemerintah, serta literatur akademik yang relevan dengan topik penelitian. Wawancara dilakukan secara semi-terstruktur untuk mendapatkan informasi lebih fleksibel dan mendalam dari informan, sedangkan observasi dilakukan untuk mengamati langsung implementasi kebijakan keamanan data di lapangan.

Analisis data dilakukan menggunakan metode Miles dan Huberman, yang mencakup tiga tahapan utama, yaitu reduksi data, penyajian data, dan penarikan kesimpulan. Reduksi data dilakukan dengan menyaring dan mengorganisasi informasi yang telah dikumpulkan agar lebih terstruktur. Penyajian data dilakukan dalam bentuk deskripsi naratif untuk menggambarkan kondisi keamanan data di Puskesmas Jabung secara sistematis. Selanjutnya, penarikan kesimpulan dilakukan dengan menginterpretasikan hasil analisis guna memahami sejauh mana prinsip kerahasiaan, integritas, dan ketersediaan telah diterapkan serta potensi perbaikannya.

HASIL DAN PEMBAHASAN

1. Mengidentifikasi Keamanan Data Rekam Medis Elektronik ditinjau dari Aspek Kerahasiaan.

Kerahasiaan data rekam medis elektronik (RME) adalah upaya untuk menjaga informasi kesehatan pasien agar hanya dapat diakses oleh pihak yang berwenang dan tidak disalahgunakan. Rekam medis elektronik berisi data pribadi yang sangat sensitif, seperti riwayat penyakit, diagnosis, hasil laboratorium, dan pengobatan yang diterima pasien (Manela et al., 2024). Oleh karena itu, perlindungan terhadap informasi ini sangat penting untuk menjaga hak privasi pasien serta mencegah penyalahgunaan data. Hal tersebut didukung oleh pernyataan informan berikut:

"*Kami menerapkan sistem manajemen hak akses yang ketat. Hanya tenaga medis yang berwenang yang dapat mengakses data pasien sesuai dengan tugasnya. Juga, setiap akses ke sistem tercatat dalam audit log untuk memantau aktivitas yang mencurigakan.*" (w.pi).

Berdasarkan hasil wawancara dan observasi yang telah dilakukan, diketahui bahwa sistem keamanan di Puskesmas Jabung sebaian masih bergantung pada pengaturan default yang disediakan oleh vendor aplikasi. Hal ini menunjukkan bahwa pengelolaan keamanan belum sepenuhnya dikendalikan secara mandiri oleh pihak internal, sehingga sebagian besar kebijakan terkait perlindungan data dan akses sistem masih mengikuti standar yang telah ditetapkan oleh vendor.

Salah satu kebijakan yang diterapkan adalah perubahan password E-Pus setiap tiga bulan sekali, yang dilakukan secara otomatis oleh vendor. Kebijakan ini dirancang sebagai langkah mitigasi risiko untuk menjaga keamanan sistem serta mengurangi kemungkinan kesalahan manusia dalam pengelolaan kredensial akses. Secara teknis, perubahan password sebenarnya dapat dilakukan secara manual dengan frekuensi yang lebih sering, misalnya sebulan sekali atau bahkan setiap minggu. Namun, penerapan perubahan otomatis setiap tiga bulan dianggap sebagai solusi terbaik yang menyeimbangkan antara aspek keamanan dan kemudahan operasional. Jika perubahan dilakukan terlalu sering, pengguna mungkin akan kesulitan mengingat password baru, yang berpotensi menyebabkan kesalahan seperti lupa password atau menggunakan pola yang mudah ditebak demi kenyamanan. Dengan kebijakan ini, sistem tetap terlindungi dari ancaman akses tidak sah tanpa memberikan beban berlebih kepada pengguna dalam hal pengelolaan kredensial.

Sedangkan untuk hak akses dalam sistem E-Pus dipetakan sesuai dengan kebutuhan masing-masing poli untuk memastikan bahwa setiap tenaga medis hanya dapat mengakses data yang relevan dengan bidangnya. Pendekatan ini bertujuan untuk mencegah terjadinya pencampuran data antar-poli, menjaga kerahasiaan rekam medis pasien, serta meningkatkan efisiensi dalam pengelolaan informasi kesehatan. Dengan sistem hak akses yang terstruktur, risiko kebocoran data dan kesalahan

administrasi dapat diminimalkan, sehingga integritas dan keamanan data pasien tetap terjaga. Hal tersebut berdasarkan pernyataan informan berikut:

"Kalau untuk hak akses itu saya siapkan tiap ruangan, jadi ID-nya itu per-ruangan, misal ini poli umum gitu ya poli umum cuma bisa ngakses yang dibutuhkan poli umum, kayak misal surat catin atau surat rujukan. Jadi kalau untuk poli gigi kan otomatis ga bisa masuk di poli umum, jadi udah saya sesuaikan dengan porsinya masing-masing." (w.pi).

Dalam upaya meningkatkan keamanan sistem informasi di Puskesmas Jabung, salah satu kebijakan yang diterapkan adalah membatasi kepemilikan dan akses terhadap perangkat komputer hanya kepada pemilik ruangan. Kebijakan ini bertujuan untuk memastikan bahwa perangkat yang digunakan untuk mengakses data pasien atau sistem rekam medis elektronik tetap berada dalam kendali orang yang bertanggung jawab secara langsung. Dengan cara ini, potensi akses tidak sah atau penggunaan komputer oleh pihak yang tidak berkepentingan dapat dikurangi, lebih dari itu Puskesmas Jabung melakukan pengadaan ID khusus Dokter yang digunakan sebagai autentikasi keamanan tambahan. Dengan adanya ID khusus ini, setiap dokter memiliki kredensial pribadi yang mana hal tersebut memberikan keamanan lebih dalam mengakses dan teridentifikasi secara personal sehingga kebijakan tersebut dapat meminimalisirkan ancaman terhadap keamanan data rekam medis dan mencegah akses tidak sah.

Dalam aspek kerahasiaan, sistem rekam medis elektronik di Puskesmas Jabung telah menerapkan pembatasan akses berbasis poli dengan penggunaan username dan password. Namun, kelemahan masih ditemukan, seperti tidak adanya fitur log out otomatis, yang memungkinkan akun tetap aktif saat komputer dihidupkan kembali tanpa perlu autentikasi ulang. Hal ini berisiko terhadap akses tidak sah dan penyalahgunaan data pasien. Meskipun hak akses pengguna telah ditetapkan secara spesifik untuk tiap poli, tanpa mekanisme pengamanan tambahan seperti autentikasi dua faktor atau sesi login yang dibatasi waktu, potensi pelanggaran kerahasiaan tetap ada. Hal ini sesuai dengan penelitian Rani et al (2024), yang menemukan bahwa meskipun pembatasan akses melalui ID dan password serta pengendalian akses internet telah diterapkan, masih diperlukan langkah lebih lanjut untuk memastikan efektivitas kebijakan tersebut seperti penerapan sistem autentikasi ganda *(multi-factor authentication)*. Langkah ini akan meningkatkan keamanan akses data pasien, mengurangi risiko pelanggaran keamanan akibat pencurian atau penyalahgunaan kredensial.

2. Mengidentifikasi Keamanan Data Rekam Medis Elektronik ditinjau dari Aspek Integritas.

Dalam hal keamanan, integritas merujuk pada upaya untuk memastikan bahwa data medis tetap akurat, utuh, tidak berubah tanpa izin, dan dapat dipercaya oleh tenaga medis maupun pasien. Menjaga integritas ini sangat penting karena data yang tidak valid atau telah dimanipulasi dapat berakibat fatal bagi pengambilan keputusan medis. Seperti menerapkan sistem audit log dalam rekam medis elektronik (RME). Di Puskesmas Jabung ini sebenarnya sudah diterapkan, tetapi hanya mencatat pengeditan data terakhir dari rekam medis pasien, bukan daftar lengkap aktivitas login pengguna. Artinya, sistem ini lebih berfokus pada perubahan yang dilakukan terhadap data pasien daripada mencatat siapa saja yang masuk ke dalam sistem dan kapan mereka mengaksesnya. Hal tersebut berdasarkan pernyataan informan berikut:

"*Itu ada lognya, cuma bukan ter-list gitu ngga, tapi kita harus masuk dulu ke data rekam medis pasien itu terakhir pengeditan oleh siapa, jadi gitu aja sih ga ada kayak list atau kayak terakhir log in itu siapa, itu belum ada untuk E-puskesmasnya sendiri.*" (w.pi)

Selain itu, akses terhadap audit log ini dibatasi secara ketat. Hanya penanggung jawab masing-masing poli yang sudah ditetapkan sebelumnya yang dapat melihat riwayat perubahan data tersebut. Pengaturan ini bertujuan untuk menjaga keamanan dan integritas data pasien serta memastikan bahwa setiap perubahan dilakukan oleh pihak yang memang memiliki kewenangan. Hal ini sesuai dengan pernyataan informan sebagai berikut:

"*Karena untuk log in yang tau passwordnya adalah penanggungjawab ruangan, jadi kayak misal pasien poli gigi gitu, kalau datanya mau diubah itu harus log in ke poli gigi, dan dia harus tanya ke penanggungjawabnya, jadi menurut saya itu sudah sangat kuat dan sangat aman karena itu menyangkut masalah tanggung jawab, jadi itu udah masing-masing polinya sendiri sih.*" (w.pi)

Merujuk pada pernyataan informan tersebut, peneliti dapat mengungkapkan Integritas ini sangat penting untuk memastikan bahwa informasi medis yang digunakan oleh tenaga kesehatan tetap valid, tidak berubah tanpa izin, dan dapat dipercaya dalam pengambilan keputusan medis. Lebih dari itu, sudut pandang peneliti beranggapan bahwa aspek integritas dalam keamanan data di Puskesmas Jabung telah diterapkan melalui sistem audit log yang mencatat pengeditan terakhir data rekam medis pasien. Namun, jika dibandingkan dengan konsep integritas dalam teori keamanan data, sistem yang ada masih memiliki keterbatasan. Idealnya, audit log tidak hanya mencatat perubahan data pasien, tetapi juga harus merekam seluruh aktivitas pengguna, termasuk waktu login, akses terhadap data, serta tindakan yang dilakukan dalam sistem. Dengan sistem yang saat ini diterapkan di Puskesmas Jabung, hanya perubahan terakhir yang tercatat, sehingga sulit untuk melakukan pelacakan jika terjadi aktivitas mencurigakan sebelum perubahan tersebut terjadi.

Dalam aspek integritas, sistem telah menerapkan audit log untuk mencatat perubahan data rekam medis elektronik, tetapi hanya mencatat perubahan terakhir tanpa menyertakan daftar lengkap aktivitas pengguna. Hal ini menyebabkan kesulitan dalam melacak riwayat akses dan modifikasi data secara menyeluruh, yang dapat berisiko jika terjadi penyalahgunaan atau manipulasi informasi medis. Selain itu, hak akses untuk mengedit data hanya diberikan kepada penanggung jawab tiap poli, yang sudah sesuai dengan prinsip keamanan data. Hal tersebut juga sejalan dengan penelitian Tri Ardianto et al (2024), bahwa di dalam sistem E-RM sudah terdapat fitur edit yang hanya dapat digunakan oleh petugas sesuai dengan hak aksesnya berdasarkan tugas, wewenang dan tanggung jawabnya. Namun, untuk meningkatkan integritas data, perlu adanya pencatatan aktivitas pengguna yang lebih detail dalam audit log, termasuk waktu login, tindakan yang dilakukan, dan perubahan data dari setiap sesi pengguna. Dengan demikian, sistem akan lebih transparan dan risiko manipulasi data dapat diminimalkan.

3. Mengidentifikasi Keamanan Data Rekam Medis Elektronik ditinjau dari Aspek Ketersediaan.

Ketersediaan data rekam medis elektronik merupakan jaminan data dan informasi yang ada dalam rekam medis elektronik dapat diakses dan digunakan oleh orang yang telah memiliki hak akses yang ditetapkan oleh pimpinan fasilitas pelayanan kesehatan (Tri Ardianto et al., 2024). Ketersediaan ini sangat penting dalam sistem kesehatan modern karena berpengaruh langsung pada kecepatan, efisiensi, dan akurasi layanan kesehatan. Dengan sistem yang selalu tersedia, tenaga medis dapat segera mengambil keputusan yang tepat untuk perawatan pasien, terutama dalam situasi darurat.

Dalam sistem keamanan rekam medis elektronik (RME) di Puskesmas Jabung, ketersediaan data dijamin dengan sistem backup otomatis ke cloud. Hal ini dilakukan melalui kerja sama dengan pihak tertentu yang bertanggung jawab terhadap pengelolaan infrastruktur cloud. Tujuan utama dari backup otomatis ini adalah untuk menjamin keberlanjutan layanan, memastikan bahwa data pasien tetap tersedia dan aman jika terjadi gangguan teknis atau kehilangan data pada sistem lokal. Didasarkan pada pernyataan informan berikut:

"*Ini sistemnya adalah cloud dan ini juga udah kerjasama dengan telkom, dan saya sudah memastikan itu saya yakin 100% kalau data ini akan ter-backup selama kita masih mengikuti kontrak tersebut. Untuk masalah proses mem-backupnya kalau cloud ya otomatis secara real time, jadi begitu data dirubah sekarang ya otomatis akan menyimpan sekarang juga.*" (w.pi)

Dalam menghadapi gangguan server atau bencana yang mengakibatkan terganggunya akses ke sistem rekam medis elektronik di Puskesmas jabung, sistem telah memiliki mekanisme pemulihan data yang memungkinkan penyimpanan sementara secara lokal. Jika terjadi gangguan server, data pasien secara otomatis disimpan dalam perangkat lokal hingga server kembali berfungsi. Setelah server aktif kembali, data yang tertunda akan dikirim secara bersamaan ke cloud, dengan notifikasi yang menunjukkan data mana saja yang belum terkoneksi atau belum tersimpan di server pusat.

Selain itu, sistem berbasis web yang digunakan memungkinkan akses dari berbagai perangkat, termasuk komputer, laptop, maupun ponsel. Oleh karena itu, apabila terjadi kerusakan pada perangkat keras, akses ke sistem tetap dapat dilakukan dari perangkat lain selama pengguna memiliki kredensial login yang sesuai. Hal ini menunjukkan bahwa sistem yang diterapkan memiliki fleksibilitas tinggi dalam mengatasi kendala perangkat keras, sehingga risiko kehilangan akses akibat kerusakan perangkat dapat diminimalkan. Penyataan tersebut mengacu pada perkataan informan sebagai berikut:

"*Kalau misal ada kerusakan perangkat keras itu juga belum pernah, maksudnya kan ini sistemnya web ya, jadi meskipun saya pakai handphone, pakai laptop, pakai komputer berbeda-beda, tapi kalau misal saya login sesuai dengan yang saya maksud, misal nih saya login poli umum saya loginkan di komputer luar gitu lah, laptop pribadi gitu, ya bisa bisa aja selama ini sesuai dengan loginnya, jadi ga masalah kalau ada kerusakan perangkat keras.*" (w.pi)

"*Karena penggunaannya berbasis web, jadi gampang di operasikan misal diluar Puskesmas juga bisa, ataupun ketika listrik mati bisa dibuka di HP. Sejauh ini aman, selalu bisa diakses ketika dibutuhkan.*" (w.krm)

Berdasarkan dari hasil peneliti, sistem yang diterapkan di Puskesmas Jabung dalam menjamin ketersediaan data rekam medis elektronik telah menunjukkan kesiapan dalam menghadapi gangguan teknis maupun bencana yang dapat menghambat akses terhadap informasi medis. Mekanisme backup otomatis cloud menjadi langkah strategis dalam memastikan data tetap tersedia serta untuk melindungi data akademik dari ancaman eksternal, bahkan ketika terjadi gangguan pada sistem lokal (Amrullah et al., 2025). Hal ini sesuai dengan prinsip dalam teori keamanan data, dimana aspek ketersediaan harus didukung oleh infrastruktur yang memungkinkan pemulihan data dengan cepat dan efisien.

Dalam aspek ketersediaan, sistem telah menggunakan mekanisme pencadangan otomatis ke cloud untuk memastikan data tetap tersedia meskipun terjadi gangguan teknis atau bencana. Puskesmas Jabung bekerja sama dengan penyedia layanan cloud untuk menjamin ketersediaan data secara real-time, sehingga informasi medis dapat diakses kapan saja oleh tenaga kesehatan yang berwenang. Menurut Sofia et al (2022) ketersediaan merupakan aspek yang menekankan bahwa informasi ketika dihubungkan oleh pihak-pihak yang terkait tersedia secara cepat. Selain itu, sistem berbasis web yang diterapkan memungkinkan akses dari berbagai perangkat, seperti komputer, laptop, dan ponsel, yang mempercepat respons dalam layanan kesehatan. Namun, ketergantungan pada koneksi internet menjadi tantangan tersendiri, terutama jika terjadi gangguan jaringan. Oleh karena itu, perlu adanya mekanisme cadangan berbasis lokal yang dapat menyimpan data sementara hingga koneksi pulih, sehingga ketersediaan data tetap terjaga secara optimal.

SIMPULAN

Hasil penelitian ini dapat disimpulkan bahwa keamanan data dalam rekam medis elektronik (RME) di Puskesmas Jabung Malang telah diterapkan berdasarkan aspek kerahasiaan, integritas, dan ketersediaan, namun masih terdapat beberapa kelemahan yang perlu diperbaiki. Dalam aspek kerahasiaan, sistem telah menerapkan mekanisme pembatasan akses berbasis poli menggunakan username dan password, namun belum memiliki fitur logout otomatis, yang berpotensi meningkatkan risiko akses tidak sah terhadap data pasien. Dalam aspek integritas, keamanan data sudah cukup

terjaga karena pengeditan hanya dapat dilakukan oleh pengguna yang memiliki hak akses sesuai tugasnya, serta telah dilengkapi dengan audit log untuk mencatat perubahan data. Namun, audit log ini hanya mencatat perubahan terakhir tanpa menyimpan riwayat lengkap aktivitas pengguna. Dalam aspek ketersediaan, sistem telah menggunakan backup otomatis ke cloud untuk menjaga keberlanjutan akses data, tetapi masih terdapat kendala dalam pemulihan data saat terjadi gangguan server.

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih kepada Kepala Puskesmas Jabung, staf rekam medis, petugas IT, serta seluruh tenaga kesehatan yang telah bersedia menjadi informan dan memberikan dukungan selama proses pengumpulan data. Ucapan terima kasih juga disampaikan kepada dosen pembimbing atas bimbingan dan arahannya selama pelaksanaan penelitian ini.

DAFTAR PUSTAKA

Amrullah, Muhamad, alva hendi, & Nasiri, A. (2025). PERANCANGAN TATA KELOLA DATA MENGGUNAKAN COBIT 2019 UNTUK PENINGKATAN KETERSEDIAAN DAN KEHANDALAN DATA. *Jurnal Manajemen Informatika & Sistem Informasi (MISI)*, *8*, 142–153.

Kemenkes RI. (2022). Peraturan Menteri Kesehatan RI No 24 Tahun 2022 Tentang Rekam Medis, 33(1), 1–12.

Manela, C., Sawitri, R., Prawestiningtyas, E., Forensik, D., Kedokteran, F., & Andalas, U. (2024). *Analisis Tanggung Jawab Medis Era Rekam Medis Elektronik di Indonesia Analysis of Medical Liabilty in the Electronic Medical Record era in Indonesia*. *10*, 301–310.

Prisusanti, R. D., & Afifah, L. (2022). *Tinjauan Yuridis : Tantangan Kerahasiaan Rekam Medis Elektronik Berdasarkan pada Permenkes Nomor 24 Tahun 2022 Juridical Review : Challenges for Confidentiality of Electronic Medical Records Based on Minister of*. *24*, 258–266.

Rani, D. M., Widyaningrum, B. N., Rizqulloh, L., Bina, P., & Semarang, T. (2024). *EDUKASI MENGENAI ASPEK KEAMANAN INFORMASI DATA PASIEN EDUCATION ON INFORMATION SECURITY ASPECTS OF PATIENT*. 115–120.

Sofia, S., Ardianto, E. T., Muna, N., & Sabran, S. (2022). Analisis Aspek Keamanan Informasi Data Pasien Pada Penerapan RME di Fasilitas Kesehatan. *Jurnal Rekam Medik & Manajemen Informasi Kesehatan*, *1*(2), 94–103. https://doi.org/10.47134/rmik.v1i2.29

Sugiyono. (2022). KUANTITATIF, KUALITATIF, DAN R&D (C. ALFABETA (ed.); 29th ed.). ALFABETA.

Suhariyono, U. S., Rusdian Ikawati, F., & Afifah, N. (2025). Analisis Aspek Keamanan Informasi Data Pasien pada Rekam Medis Elektronik di UPT Puskesmas Karangploso. *Jurnal Manajemen Informasi Kesehatan Indonesia*, *13*(1), 2337–2585.

Tri Ardianto, E., Nurjanah, L., Studi Manajemen Informasi Kesehatan, P., Kesehatan, J., & Negeri Jember, P. (2024). *ANALISIS ASPEK KEAMANAN DATA PASIEN DALAM IMPLEMENTASI REKAM MEDIS ELEKTRONIK DI RUMAH SAKIT X*. *3*(2), 2829–4777. https://doi.org/10.47134/rammik.v3i2.54

Widiyanti, S. W., Hastuti, N. M., Kusumawati, E. A., Karanganyar, M. H., Brigjen, J., Barat, K., Indah, G. P., Kec, P., Karanganyar, K., & Tengah, J. (2024). *Indonesian Journal of Health Information Management (IJHIM) Vol . 4 No . 2 (2024), 1 Tinjauan Keamanan Data Rekam Medis Elektronik P a d a A p l i k a s i S i m p u s B e r d a s a r k a n A s p e k Confidentiality , Integrity , Dan Availability Di Pu*. *4*(2), 1–6.