E-ISSN: 3025-0994
Halaman 2228-2239
Volume 4 Nomor 4 Tahun 2026

Analisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik (RME) di Puskesmas Limboto

Natasya I. Umo[1], Gladis A. Ismail[2], Merlin Abd. Rahman[3]

[1,2,3] Program Studi Rekam Medis dan Informasi Kesehatan, STIKES Bakti Nusantara Gorontalo
e-mail: natasyaumo276@gmail.com

Abstrak

Keamanan data pasien merupakan salah satu aspek penting dalam penyyelengaraan Rekam Medis Eletronik (RME) karena data Kesehatan Mengandung Infromasi pribadi Yang bersifat rahasia dan sensitive. Penerapan RME di fasilitas pelayanan Kesehatan perlu didukung dengan system keamanan informasi yang mampu melindungi data dari akses yang tidak berwenang, perubahan data, maupun penyalagunaan informasi. Penelitian ini bertujuan untuk menganalisis aspek keamanan data pasien dalam implementasi Rekam Medis Eletronik (RME) di puskesmas limboto berdasarkan enam aspek kemanan informasi, yaitu kerahasiaan (confidentiality), Integritas (integrity), autentikasi (authentication), ketersediaan (availability), pengendalian akses (access control), dan nir-sangkal (non repudiation). Penelitian ini menggunakan metode deskriptif dengan pendekatan kualitatif. Informan dipilih menggunakan Teknik purposive sampling berdasarkan pengetahuan, pengalaman, dan keterlibatan dalam implementasi RME. Data dikumpulkan melalui observasi, wawancara, dan dokumentasi, kemudian dianalisis secara kualitatif melalui tahapan penyajian data serta penarikan Kesimpulan dan verivikasi. Hasil penelitian menunjukkan bahwa keenam aspek keamanan informasi telah diterapkan di puskemas limboto. Kerahasiaan didukung pembatasan akses dan pengamanan jaringan, integritas melalui vaalidasi serta audit trail, autentikasi melalui akun pengguna, ketersediaan melalui perangkat, jaringan, backup, UPS dan Genset, pengendalian akses melalui pembagian hak berdasrakan peran, serta nir-sangkal melalui audit trail, identitas petugas, PIN atau tanda tangan eletronik. Meskipun demikian, diperlukan evaluasi berkala, peningkatan, peningkatan kapasitas petugas, dan penguatan teknoloi keamanan untuk mengoptimalkan perlidungan data pasien.

Kata kunci: Autentikasi, Keamanan Data Pasien, Pengendalian akses, Rekam Medis Elektronik, Sistem Informasi.

Abstract

Patient data security is a critical aspect of Impelementing Electronic Healt Records (EHRs) because healt data contains confidential and sensitive personal information. The implementation of EHRs In healtcare facilities must be supported by an information security

system capable of protecting data from unauthorized access, data tampering, and misuse of information. This study aims to analyze aspects of patient data security in the implementation of electronic medical records (EMR) at the limboto sommunity health center based on six aspects of information security, namely confindentiality, integrity, authentication, availability, access control, and non- repudiation. This study employed a descriptive meyhod with a qualitative approach. Informants were selected using purposive sampling based on their knowledge, experience, and involvement in the EHR implementation. Data were collected through observation, interviews, and documentation, then qualitatively analyzed through the stages of data presentation, conclusion drawing, and verification. The results of the study indicate that all six aspects of information security have been implemented at the limboto community Health center. Confidentiality is supported by access restriction and network security; Integrity through validation and audit trails; authentication through user accounts; availability through devices, network, backups, UPS, and generators; access rights; and non-repudiation throught audit trails, staff indentification, PINs, or electronic signature. Nevertheless, staff capacity building, and the strengthening of security technologies are necessary to optimize the protection of patient data.

Keywords : *Authentication, Patient Data Security, Access Control, Electronic Health Records, Information Systems*

LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi digital di berbagai sektor kehidupan, termasuk sektor kesehatan. Transformasi digital dalam pelayanan kesehatan bertujuan meningkatkan mutu layanan melalui pemanfaatan teknologi informasi yang mampu mendukung efisiensi, efektivitas, keamanan, serta kesinambungan pelayanan kesehatan. Salah satu bentuk implementasi transformasi digital tersebut adalah penerapan Rekam Medis Elektronik (RME), yaitu sistem yang digunakan untuk mengelola informasi kesehatan pasien secara elektronik sehingga memudahkan penyimpanan, pengelolaan, dan pertukaran data antar fasilitas pelayanan kesehatan. Penerapan RME diharapkan mampu meningkatkan kualitas pelayanan, mempercepat akses informasi pasien, mengurangi kesalahan pencatatan, serta mendukung pengambilan keputusan klinis yang lebih akurat dan tepat waktu (Maulaningrum et al, 2025).

Sebagai bagian dari upaya transformasi sistem kesehatan nasional, Pemerintah Indonesia menetapkan kebijakan digitalisasi pelayanan kesehatan melalui penerapan Rekam Medis Elektronik (RME). Kebijakan tersebut diatur dalam Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis yang mewajibkan seluruh fasilitas pelayanan kesehatan menyelenggarakan Rekam Medis Elektronik paling lambat pada 31 Desember 2023. Implementasi RME merupakan salah satu strategi pemerintah untuk mewujudkan sistem pelayanan kesehatan yang terintegrasi, efektif, efisien, dan berorientasi pada pasien. Melalui RME, data kesehatan pasien dapat didokumentasikan secara elektronik, dikelola secara lebih akurat, serta dipertukarkan antar fasilitas pelayanan kesehatan melalui interoperabilitas sistem sehingga mendukung kesinambungan pelayanan kesehatan. Seiring

dengan meningkatnya pemanfaatan teknologi digital dalam pelayanan kesehatan, perlindungan terhadap keamanan dan kerahasiaan data pasien menjadi aspek yang sangat penting untuk menjamin kepercayaan masyarakat serta menjaga kualitas pelayanan kesehatan (Permenkes RI No 24, 2022).

Meskipun penelitian tersebut telah memberikan gambaran mengenai implementasi Rekam Medis Elektronik dan keamanan informasi, sebagian besar masih berfokus pada penerapan sistem, evaluasi kebijakan, atau hanya mengkaji sebagian aspek keamanan informasi. Belum banyak penelitian yang menganalisis secara komprehensif enam aspek keamanan informasi, yaitu *confidentiality, integrity, authentication, availability, access control,* dan *non-repudiation* dalam implementasi Rekam Medis Elektronik di tingkat puskesmas. Selain itu, berdasarkan penelusuran penelitian yang telah dilakukan, belum ditemukan penelitian yang secara khusus mengkaji keenam aspek tersebut pada implementasi Rekam Medis Elektronik di Puskesmas Limboto. Oleh karena itu, penelitian ini dilakukan untuk menganalisis aspek keamanan data pasien dalam implementasi Rekam Medis Elektronik di Puskesmas Limboto sehingga diharapkan dapat memberikan gambaran mengenai kondisi keamanan sistem yang telah diterapkan sekaligus menjadi bahan masukan bagi peningkatan keamanan data pasien di fasilitas pelayanan Kesehatan (Indriyajati et al., 2024).

METODE

Penelitian ini menggunakan metode kualitatif deskriptif. Proses pengumpulan data diperoleh dari wawancara, observasi dan dokumentasi. Sumber data pada penelitian ini yaitu data primer berupa hasil wawancara dan observasi langsung di tempat penelitian, serta data sekunder adalah data yang diperoleh secara tidak langsung melalui jurnal dan article. Analisis data yang digunakan dalam penelitian ini Adalah penyajian data dan penarikan kesimpulan.

HASIL

Tabel 1 karakteristik informan penelitian

No	Inisial	Umur	Jabatan	Status informan
1	H.T	52 Tahun	Kepala puskesmas	Infroman kunci
2	S.Y.A	40 Tahun	Admin Sistem RME	Informan utama
3	D	38 Tahun	Petugas rekam medis	Informan utama
4	A	24 Tahun	Perawat	Informan tambahan
5	A.A.L	27 Tahun	Dokter	Informan tambahan

Penerapan Aspek Kerahasiaan (Confidentiality)

Berdasarkan hasil penelitian Dan hasil wawancara dengan infroman di Puskesmas dapat disimpulkan bahwa penerapan aspek kerahasiaan (confidentiality) di Puskesmas Limboto telah dilakukan melalui perlindungan tampilan informasi pada komputer, penerapan kewajiban menjaga kerahasiaan data oleh seluruh petugas, serta pengamanan database Rekam Medis Elektronik menggunakan jaringan lokal dengan pembatasan akses, sehingga kerahasiaan informasi pasien dapat terjaga dengan baik.

Penerapan Aspek Integritas (Integrity)

Berdasarkan hasil penelitian dan hasil wawancara dengan informan dapat disimpulkan bahwa penerapan aspek integritas (integrity) di Puskesmas Limboto telah dilakukan melalui validasi data saat proses input, penguncian data rekam medis setelah disimpan oleh dokter, serta pencatatan setiap perubahan data melalui audit trail. Mekanisme tersebut mendukung keakuratan, keutuhan, dan keamanan data Rekam Medis Elektronik dari perubahan yang tidak sah.

Penerapan Aspek Autentikasi (Authentication)

Berdasarkan hasil penelitian dan hasil wawancara informan dapat disimpulkan bahwa penerapan aspek autentikasi (authentication) di Puskesmas Limboto telah dilakukan melalui penggunaan akun pengguna yang bersifat individual, penerapan penghentian sesi otomatis (session timeout), serta pengelolaan kata sandi secara berkala. Mekanisme tersebut memastikan bahwa akses ke sistem Rekam Medis Elektronik hanya dapat dilakukan oleh pengguna yang telah terverifikasi dan memiliki kewenangan sesuai tugasnya.

Penerapan Aspek Ketersediaan (Availability)

Berdasarkan hasil penelitian dan hasil wawancara dengan infroman dapat disimpulkan bahwa penerapan aspek ketersediaan (availability) di Puskesmas Limboto telah didukung oleh penyediaan perangkat komputer dan jaringan yang terintegrasi, pelaksanaan pencadangan data secara berkala, serta penyediaan UPS dan genset sebagai sumber daya cadangan. Upaya tersebut bertujuan untuk memastikan sistem Rekam Medis Elektronik tetap tersedia dan dapat diakses secara berkelanjutan dalam mendukung pelayanan kepada pasien.

Penerapan Aspek Pengendalian Akses (Access Control)

Berdasarkan Hasil penelitian dan wawancara dapat diketahui bahwa aspek akses kontrol dalam implementasi RME di Puskesmas Limboto telah diterapkan dengan baik. Hal ini ditunjukkan melalui adanya pembagian hak akses, penggunaan role pengguna, pembatasan akses berdasarkan tugas dan kewenangan, serta penggunaan akun pengguna dalam mengakses sistem. Penerapan tersebut telah mendukung upaya perlindungan terhadap data pasien karena akses terhadap informasi rekam medis tidak diberikan secara bebas kepada seluruh pengguna.

Penerapan Aspek Nir Sangkal (Non-Repudiation)

Berdasarkan hasil penelitian dan hasil wawancara SYA,AAL, dan SYA dapat disimpulkan bahwa penerapan aspek pengendalian akses di Puskesmas Limboto telah didukung oleh pencatatan aktivitas pengguna melalui audit trail, pencantuman identitas petugas penanggung jawab pada setiap dokumen rekam medis, serta penggunaan PIN atau Tanda Tangan Elektronik (TTE) sebagai mekanisme pengesahan dokumen. Penerapan tersebut mendukung pengawasan terhadap akses dan penggunaan sistem Rekam Medis Elektronik serta meningkatkan keamanan dan akuntabilitas pengelolaan data pasien.

PEMBAHASAN

Penerapan Aspek Kerahasiaan (Confidentiality)

Berdasarkan Hasil penelitian menunjukkan bahwa aspek kerahasiaan (confidentiality) pada implementasi Rekam Medis Elektronik (RME) di Puskesmas Limboto diwujudkan melalui pengaturan posisi layar komputer pada bagian pendaftaran dan ruang pemeriksaan agar tidak dapat dilihat oleh pasien maupun pengunjung lain, penerapan kewajiban seluruh petugas untuk menjaga kerahasiaan data pasien sesuai regulasi dan kode etik profesi, serta pengamanan basis data RME menggunakan jaringan lokal (Local Area Network) yang dibatasi aksesnya dari luar. Ketiga mekanisme tersebut menunjukkan bahwa perlindungan kerahasiaan dilakukan baik secara fisik maupun secara sistem digital.

Temuan tersebut sejalan dengan prinsip keamanan informasi dalam ISO/IEC 27001 yang menegaskan bahwa kerahasiaan menjamin informasi hanya dapat diakses oleh pihak yang berwenang, serta selaras dengan ketentuan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 dan Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan yang mewajibkan fasilitas pelayanan kesehatan menjamin kerahasiaan data pasien. Hasil ini juga konsisten dengan penelitian terdahulu yang menyatakan bahwa perlindungan kerahasiaan data pasien umumnya dilakukan melalui pembatasan akses sistem, penggunaan jaringan internal, serta penerapan etika profesi tenaga kesehatan, dan dengan kajian yang menekankan bahwa keamanan data pasien tidak hanya bergantung pada teknologi, tetapi juga pada kepatuhan petugas terhadap aturan kerahasiaan informasi. Selain itu, Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan serta Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 (Pemerintah Republik Indonesia, 2023) Rekam Medis juga menegaskan bahwa fasilitas pelayanan kesehatan wajib menjamin kerahasiaan data pasien selama proses penyelenggaraan rekam medis elektronik. Keshta dan Odeh (2021) serta Tertulino et al. (2024) juga menggarisbawahi pentingnya kebijakan privasi dan pembatasan akses pada sistem rekam medis elektronik.

Hasil penelitian ini sejalan dengan penelitian (Alzoubi et al., 2026) yang menyatakan bahwa perlindungan kerahasiaan data pasien dilakukan melalui pembatasan akses sistem, penggunaan jaringan internal, serta penerapan etika profesi oleh seluruh tenaga kesehatan. Penelitian (WHO, 2019) juga menunjukkan bahwa perlindungan data pasien tidak hanya bergantung pada teknologi, tetapi juga pada kepatuhan petugas terhadap aturan kerahasiaan informasi.

Menurut peneliti, penerapan aspek kerahasiaan di Puskesmas Limboto telah berjalan dengan baik. Pengaturan tata ruang pelayanan, pembatasan jaringan, serta komitmen petugas mencerminkan adanya kesadaran terhadap pentingnya melindungi data pasien. Namun demikian, peneliti berpandangan bahwa penguatan lebih lanjut masih diperlukan, misalnya melalui penerapan enkripsi data dan autentikasi berlapis (multi-factor authentication), agar risiko kebocoran data dapat ditekan seminimal mungkin. Temuan lintas studi tentang privasi RME juga dapat dibaca dalam Alkhatib et al. (2024).

Penerapan Aspek Integritas (Integrity)

Berdasarkan Hasil penelitian menunjukkan bahwa aspek integritas (integrity) diterapkan melalui validasi data pada saat proses input menggunakan menu pilihan (drop-down) sesuai standar ICD-10 serta validasi Nomor Induk Kependudukan (NIK), penguncian data (locking system) secara otomatis setelah rekam medis diverifikasi dan disimpan oleh dokter, serta pencatatan seluruh aktivitas perubahan data melalui audit trail yang merekam waktu dan akun pengguna. Mekanisme tersebut bekerja secara berjenjang mulai dari tahap input hingga penyimpanan data.

Temuan ini sejalan dengan prinsip integrity dalam ISO/IEC 27001:2022 yang menekankan bahwa informasi harus tetap akurat, lengkap, konsisten, dan terlindungi dari perubahan yang tidak sah, serta sejalan dengan ketentuan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 yang mewajibkan pengelolaan rekam medis secara benar, lengkap, dan dapat dipertanggung jawabkan. Kajian Kiani et al. (2023) dan Ettaloui et al. (2024) membahas opsi teknologi untuk menjaga integritas dan keterlacakan data kesehatan digital.

Hasil penelitian ini juga konsisten dengan kajian terdahulu yang menjelaskan bahwa validasi data, audit trail, dan pengendalian perubahan data merupakan mekanisme penting untuk menjaga integritas rekam medis elektronik, sebagaimana juga ditegaskan dalam standar ISO/IEC 27002:2022 mengenai pentingnya audit logging dalam menelusuri setiap perubahan informasi. Selain itu, Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis (Permenkes RI No 24, 2022) menegaskan bahwa data rekam medis harus dikelola secara benar, lengkap, dan dapat dipertanggungjawabkan selama proses penyelenggaraan pelayanan kesehatan (Kementerian Kesehatan RI, 2022). Ketentuan tersebut menunjukkan bahwa setiap perubahan data harus dapat ditelusuri dan dilakukan oleh petugas yang memiliki kewenangan.

Hasil penelitian ini sejalan dengan penelitian (T. A. Putri et al., 2026) yang menjelaskan bahwa penerapan validasi data, audit trail, serta pengendalian perubahan data merupakan mekanisme penting dalam menjaga integritas Rekam Medis Elektronik sehingga informasi kesehatan tetap akurat, lengkap, dan terlindungi dari perubahan yang tidak sah. Selain itu, ISO/IEC 27002:2022 menegaskan bahwa audit logging dan pengelolaan perubahan data merupakan kontrol keamanan yang diperlukan untuk memastikan setiap perubahan informasi dapat ditelusuri dan dipertanggungjawabkan.

Menurut peneliti, penerapan aspek integritas di Puskesmas Limboto sudah berjalan baik karena validasi dilakukan sejak tahap awal pengisian data, dilanjutkan dengan penguncian data setelah verifikasi dokter, dan diperkuat oleh pencatatan audit trail. Meskipun demikian, peneliti menilai perlu adanya validasi otomatis yang lebih komprehensif serta pemantauan audit trail secara berkala agar potensi kesalahan atau penyalahgunaan data dapat dicegah lebih dini.

Penerapan Aspek Autentikasi (Authentication)

Berdasarkan Hasil penelitian menunjukkan bahwa aspek autentikasi diterapkan melalui penggunaan akun pengguna yang bersifat individual (unique user ID) sehingga penggunaan akun bersama tidak diperkenankan, penerapan penghentian sesi otomatis (session timeout) ketika komputer tidak digunakan dalam jangka waktu tertentu, serta

pengelolaan kata sandi melalui imbauan penggantian secara berkala. Ketiga mekanisme ini bekerja untuk memastikan bahwa hanya pengguna terverifikasi yang dapat mengakses sistem.

Temuan tersebut sejalan dengan prinsip autentikasi dalam ISO/IEC 27001:2022 yang menempatkan verifikasi identitas pengguna sebagai syarat sebelum pemberian hak akses, serta sejalan dengan ketentuan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 yang membatasi akses RME hanya bagi tenaga kesehatan berwenang. Hasil ini juga konsisten dengan penelitian terdahulu yang menjelaskan bahwa penggunaan akun individual dan pengelolaan kredensial merupakan komponen utama untuk mencegah akses tidak sah, serta dengan kajian lain yang menegaskan bahwa identitas digital yang unik, pengelolaan kata sandi yang baik, dan penghentian sesi otomatis merupakan mekanisme autentikasi yang efektif. Selain itu, Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis (Keshri, 2017) menegaskan bahwa akses terhadap Rekam Medis Elektronik hanya dapat dilakukan oleh tenaga kesehatan dan petugas yang memiliki kewenangan sesuai tugas dan tanggung jawabnya (Kementerian Kesehatan RI, 2022). Oleh karena itu, setiap pengguna wajib memiliki identitas akun yang bersifat individual sebagai bentuk pengendalian akses terhadap data pasien. Cobrado et al. (2024) menjelaskan keterkaitan identifikasi, autentikasi, otorisasi, dan akuntabilitas dalam keamanan akses rekam medis elektronik.

Hasil penelitian ini sejalan dengan penelitian (Akmal et al., 2026) yang menjelaskan bahwa penggunaan akun individual, autentikasi pengguna, serta pengelolaan kredensial merupakan komponen utama dalam menjaga keamanan Rekam Medis Elektronik dan mencegah akses oleh pihak yang tidak berwenang. Selain itu, (Proud-madruga & Choong, 2024) menjelaskan bahwa penggunaan identitas digital yang unik, pengelolaan kata sandi yang baik, serta penghentian sesi otomatis merupakan mekanisme autentikasi yang efektif untuk meningkatkan keamanan sistem informasi.

Menurut peneliti, penerapan autentikasi di Puskesmas Limboto sudah cukup baik karena setiap pengguna memiliki identitas akun tersendiri dan sistem dilengkapi mekanisme sesi otomatis. Namun demikian, peneliti berpandangan bahwa penguatan lebih lanjut, seperti penerapan multi-factor authentication (MFA), kebijakan kata sandi yang lebih ketat, serta edukasi keamanan informasi secara berkala, masih diperlukan untuk mengurangi risiko penyalahgunaan akun. Asih et al. (2024) melaporkan bahwa perlindungan data pasien melibatkan faktor teknis, manusia, dan kepatuhan terhadap kebijakan.

Penerapan Aspek Ketersediaan (Availability)

Hasil penelitian menunjukkan bahwa aspek ketersediaan diwujudkan melalui penyediaan perangkat komputer pada seluruh unit pelayanan yang terhubung dalam jaringan lokal terintegrasi, pelaksanaan pencadangan (backup) data secara rutin ke server lokal cadangan maupun media penyimpanan eksternal, serta penyediaan UPS dan genset untuk mengantisipasi gangguan pasokan listrik. Infrastruktur tersebut mendukung agar sistem RME tetap dapat diakses selama jam pelayanan.

Temuan ini sejalan dengan prinsip availability dalam ISO/IEC 27001:2022 yang menjamin bahwa informasi dan sistem dapat diakses oleh pengguna berwenang setiap kali dibutuhkan, serta sejalan dengan ketentuan Peraturan Menteri Kesehatan Nomor 24 Tahun

2022 yang mensyaratkan dukungan infrastruktur teknologi informasi dalam penyelenggaraan RME. Hasil penelitian ini juga konsisten dengan kajian terdahulu yang menyatakan bahwa pencadangan data secara berkala dan kesiapan infrastruktur merupakan strategi penting menjaga keberlangsungan sistem kesehatan digital, serta dengan penelitian lain yang menunjukkan bahwa penyediaan sumber daya listrik cadangan dan sistem pemulihan data mampu meminimalkan gangguan pelayanan. Menurut **ISO/IEC 27001:2022**, *availability* merupakan jaminan bahwa informasi dan sistem dapat diakses oleh pengguna yang berwenang setiap kali dibutuhkan. Dalam pelayanan kesehatan, ketersediaan sistem sangat menentukan kelancaran pelayanan karena keterlambatan akses terhadap data pasien dapat memengaruhi proses diagnosis maupun tindakan medis. Selain itu, **Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis** menegaskan bahwa penyelenggaraan Rekam Medis Elektronik harus didukung oleh infrastruktur teknologi informasi yang mampu menjamin ketersediaan data selama pelayanan kesehatan berlangsung. Folasole et al. (2023) menyoroti kebutuhan mitigasi ancaman terhadap keamanan dan keberlanjutan layanan sistem rekam kesehatan elektronik.

Hasil penelitian ini sejalan dengan penelitian **(Ortiz-Mallasén et al., 2024)** yang menyatakan bahwa pencadangan data secara berkala dan kesiapan infrastruktur teknologi merupakan strategi penting dalam menjaga keberlangsungan sistem kesehatan digital. Penelitian (Sajid et al., 2024)juga menjelaskan bahwa penyediaan sumber daya listrik cadangan dan sistem pemulihan data mampu meminimalkan gangguan pelayanan akibat kegagalan sistem maupun pemadaman listrik.

Menurut peneliti, dukungan infrastruktur di Puskesmas Limboto sudah memadai untuk menjaga ketersediaan layanan RME. Meskipun demikian, peneliti menilai bahwa pemantauan jaringan secara berkala, pengujian rutin proses backup, serta evaluasi sistem pemulihan data tetap perlu dilakukan agar pelayanan tidak terganggu, terutama pada kondisi darurat atau kegagalan sistem yang tidak terduga.

Penerapan Aspek Pengendalian Akses (Access Control)

Berdasarkan Hasil penelitian menunjukkan bahwa pengendalian akses dilakukan melalui pembagian hak akses berdasarkan peran pengguna (Role-Based Access Control/RBAC), di mana petugas pendaftaran hanya dapat menginput data identitas pasien, tenaga medis dapat mengakses riwayat dan data klinis, petugas farmasi hanya dapat melihat resep elektronik, dan petugas laboratorium hanya mengakses data pemeriksaan penunjang. Sistem juga dilengkapi audit trail serta identitas penanggung jawab pada setiap dokumen

Temuan tersebut sejalan dengan prinsip access control dalam ISO/IEC 27001:2022 yang menegaskan bahwa pembatasan hak akses berdasarkan peran merupakan metode efektif menjaga keamanan sistem informasi, serta sejalan dengan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 yang membatasi akses RME hanya bagi tenaga kesehatan berwenang. Hasil penelitian ini juga konsisten dengan kajian terdahulu yang menunjukkan bahwa penerapan RBAC mampu meningkatkan keamanan sistem rekam medis elektronik melalui pembatasan hak akses berdasarkan fungsi kerja, serta dengan penelitian lain yang menegaskan bahwa audit trail dan pengelolaan hak

akses merupakan komponen penting dalam menjaga keamanan informasi kesehatan elektronik Menurut **ISO/IEC 27001:2022**, *access control* bertujuan membatasi hak akses pengguna sesuai kewenangannya sehingga risiko penyalahgunaan informasi dapat diminimalkan. Pembagian hak akses berdasarkan peran merupakan salah satu metode yang efektif dalam menjaga keamanan sistem informasi kesehatan. Selain itu, **Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022** menjelaskan bahwa akses terhadap Rekam Medis Elektronik hanya diberikan kepada tenaga kesehatan yang memiliki kewenangan sesuai tugas dan tanggung jawabnya. Nowrozy et al. (2024) menekankan bahwa perlindungan privasi memerlukan rancangan pengamanan sepanjang siklus pengelolaan dan pertukaran data kesehatan.

Hasil penelitian ini sejalan dengan penelitian **(Asmaa Abdalhadi Hisham Abdalbaset1, 2024)** yang menjelaskan bahwa penerapan **Role-Based Access Control (RBAC)** mampu meningkatkan keamanan sistem Rekam Medis Elektronik melalui pembatasan hak akses berdasarkan fungsi kerja pengguna. Penelitian **(Keshta & Odeh, 2021)** juga menyatakan bahwa *audit trail* dan pengelolaan hak akses merupakan komponen penting dalam menjaga keamanan informasi kesehatan elektronik.

Menurut peneliti, pembagian hak akses di Puskesmas Limboto telah sesuai dengan prinsip keamanan informasi karena setiap pengguna hanya dapat mengakses menu sesuai kewenangannya, sehingga risiko penyalahgunaan data dapat diminimalkan. Namun demikian, peneliti berpandangan bahwa evaluasi hak akses perlu dilakukan secara berkala agar tetap relevan dengan perubahan tugas maupun struktur organisasi di puskesmas**.**

Penerapan Aspek Nir Sangkal (Non-Repudiation)

Berdasarkan Hasil penelitian menunjukkan bahwa aspek nir sangkal diterapkan melalui pencatatan seluruh aktivitas pengguna (audit trail) yang merekam akun, jenis tindakan, serta waktu transaksi, pencantuman identitas petugas penanggung jawab pada setiap dokumen rekam medis, serta penggunaan PIN atau Tanda Tangan Elektronik pada dokumen rekam medis digital. Mekanisme tersebut memberikan bukti autentik terhadap setiap aktivitas yang dilakukan pengguna dalam system

Temuan ini sejalan dengan prinsip non-repudiation dalam ISO/IEC 27001:2022 yang menjamin bahwa seseorang tidak dapat menyangkal tindakan yang telah dilakukan dalam suatu sistem informasi, serta sejalan dengan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 yang mengatur bahwa pencatatan dan pengesahan RME harus dapat diidentifikasi berdasarkan identitas tenaga kesehatan yang bertanggung jawab. Hasil penelitian ini juga konsisten dengan kajian terdahulu yang menjelaskan bahwa audit trail, identitas digital, dan tanda tangan elektronik mampu meningkatkan prinsip non-repudiation dalam sistem rekam medis elektronik, serta dengan penelitian lain yang menegaskan bahwa pencatatan aktivitas pengguna merupakan komponen penting dalam meningkatkan akuntabilitas dan keamanan informasi Kesehatan Menurut **ISO/IEC 27001:2022**, *non-repudiation* merupakan prinsip keamanan informasi yang menjamin bahwa seseorang tidak dapat menyangkal tindakan yang telah dilakukan dalam suatu sistem informasi. Prinsip tersebut diwujudkan melalui penggunaan identitas pengguna

yang unik, *audit log*, serta tanda tangan elektronik sebagai bukti autentik terhadap setiap transaksi. Selain itu, **Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis** mengatur bahwa setiap pencatatan dan pengesahan Rekam Medis Elektronik harus dapat diidentifikasi berdasarkan identitas tenaga kesehatan yang bertanggung jawab. Pool et al. (2024) menunjukkan bahwa pencegahan insiden kebocoran data menuntut pengelolaan risiko dan tata kelola keamanan yang menyeluruh.

Hasil penelitian ini sejalan dengan penelitian **(Kerkhove et al., 2023)** yang menjelaskan bahwa penerapan *audit trail*, identitas digital, dan tanda tangan elektronik mampu meningkatkan prinsip **non-repudiation** dalam sistem Rekam Medis Elektronik sehingga setiap aktivitas pengguna dapat dipertanggungjawabkan. Penelitian(Keshta & Odeh, 2021)juga menyatakan bahwa mekanisme pencatatan aktivitas pengguna merupakan salah satu komponen penting dalam meningkatkan akuntabilitas dan keamanan informasi kesehatan.

Menurut peneliti, penerapan aspek nir sangkal di Puskesmas Limboto telah berjalan baik karena setiap aktivitas dalam sistem dapat dipertanggungjawabkan baik secara administratif maupun hukum. Meskipun demikian, peneliti menilai bahwa evaluasi terhadap pengelolaan log aktivitas serta optimalisasi penggunaan tanda tangan elektronik tersertifikasi tetap perlu dilakukan untuk memperkuat keamanan dan akuntabilitas sistem.

SIMPULAN

Berdasarkan hasil penelitian mengenai Analisis Aspek Keamanan Data Pasien dalam Implementasi Rekam Medis Elektronik (RME) di Puskesmas Limboto, dapat disimpulkan sebagai berikut: Aspek kerahasiaan *(Confidentiality)* telah diterapkan melalui pengaturan posisi layar komputer, penerapan kewajiban menjaga kerahasiaan data pasien oleh seluruh petugas sesuai kode etik dan peraturan yang berlaku, serta pengamanan database menggunakan jaringan lokal (Local Area Network/LAN). Upaya tersebut menunjukkan bahwa hanya dibatasinya kepada petugas yang memiliki kewenangan. Aspek integritas (*Integrity*) telah diterapkan melalui validasi data pada saat proses input, pengisian data, penguncian data rekam medis setelah diverifikasi oleh dokter, serta pencatatan setiap perubahan data melalui audit trail. Penerapan tersebut mendukung keakuratan, keutuhan, dan konsistensi data rekam medis elektronik. Aspek autentikasi (*Authentication*) telah diterapkan dengan penggunaan akun pengguna yang bersifat individual, penerapan session timeout, dan pengelolaan kata sandi secara berkala. Mekanisme tersebut memastikan bahwa hanya pengguna yang memiliki identitas dan kewenangan yang dapat mengakses sistem Rekam Medis Elektronik. Aspek ketersediaan (*Availability*) telah didukung oleh penyediaan perangkat komputer pada setiap unit pelayanan, jaringan lokal yang terintegrasi, pelaksanaan pencadangan (backup) data secara berkala, serta penyediaan UPS dan genset sebagai sumber daya cadangan. Penerapan tersebut mendukung keberlangsungan pelayanan kesehatan dan memastikan sistem tetap dapat digunakan ketika terjadi gangguan. Aspek pengendalian akses (*Access Control*) telah diterapkan melalui pembagian hak akses berdasarkan peran dan tugas masing-masing petugas (Role-Based Access Control/RBAC). Selain itu, sistem dilengkapi dengan audit trail, identitas penanggung jawab, serta mekanisme pengesahan dokumen

menggunakan PIN atau Tanda Tangan Elektronik sehingga mampu meningkatkan keamanan dan akuntabilitas penggunaan sistem. Aspek nir sangkal (*Non-Repudiation*) telah diterapkan melalui pencatatan aktivitas pengguna (audit trail), pencantuman identitas tenaga kesehatan pada setiap dokumen rekam medis elektronik, serta penggunaan PIN atau Tanda Tangan Elektronik sebagai bukti autentik terhadap setiap transaksi dalam sistem. Penerapan tersebut mendukung akuntabilitas, transparansi, dan kepastian hukum dalam pengelolaan Rekam Medis Elektronik di Puskesmas Limboto.

DAFTAR PUSTAKA

Abdalbaset, A. A. H. (2024). Access Control and Role-Based Access Security in Healthcare Information Systems. Journal of Cybersecurity and Data Protection, 8(2), 112–124.

Adiputra, I. M. S., Trivena, T., & Purba, D. H. (2021). Metodologi Penelitian Kesehatan. Medan: Yayasan Kita Tulis.

Akmal, M., Suryani, L., & Rahman, F. (2026). Evaluation of User Authentication and Access Control Security in Electronic Medical Record Systems. Journal of Health Informatics and Security, 12(1), 45–58.

Alkhatib, A. J., AlZoubi, A., Alaiad, A., Abu Aqoulah, A., Alawnah, A. B., Alharoun, M., & Azar, M. (2024). Privacy issues in electronic medical records: A systematic review. Multicriteria Algorithms with Applications, 3, 32–41. https://doi.org/10.61356/j.mawa.2024.311761

Alzoubi, A., Al-Khateeb, M., & Hasan, H. (2026). Confidentiality and Data Protection Standards in Electronic Health Record Implementation. International Journal of Medical Informatics, 182, 105310.

Ardianto, R., & Nurjanah, S. (2024). Sistem Informasi Kesehatan dan Tata Kelola Keamanan Data Pasien. Jakarta: Pustaka Kesehatan.

Asih, H. A., Indrayadi, I., Soraya, S., & Khairunnisa, K. (2024). Evaluasi keamanan data pasien pada rekam medis elektronik dengan systematic literature review. Jurnal Ilmiah FIFO, 16(2). https://doi.org/10.22441/fifo.2024.v16i2.001

Azahwa, S., Pratama, A., & Lestari, D. (2025). Analisis Sumber Daya Manusia dan Sarana Prasarana dalam Pengelolaan Rekam Medis di Puskesmas. Jurnal Informasi Kesehatan, 9(1), 22–31.

Cobrado, U. N., Sharief, S., Regahal, N. G., Zepka, E., Mamauag, M., & Velasco, L. C. (2024). Access control solutions in electronic health record systems: A systematic review. Informatics in Medicine Unlocked, 49, 101552. https://doi.org/10.1016/j.imu.2024.101552

Darmawan, A. (2022). Aspek Hukum dan Perlindungan Kerahasiaan Data Pasien dalam Rekam Medis Elektronik. Jurnal Hukum Kesehatan Indonesia, 4(2), 110–121.

Ettaloui, N., Arezki, S., & Gadi, T. (2024). Blockchain-based electronic health record: Systematic literature review. Human Behavior and Emerging Technologies, 2024, 4734288. https://doi.org/10.1155/hbe2/4734288

Folasole, A., Adegboye, O. S., Ekuewa, O. I., & Eshua, P. E. (2023). Security, privacy challenges and available countermeasures in electronic health record systems: A

review. European Journal of Electrical Engineering and Computer Science, 7(6). https://doi.org/10.24018/ejece.2023.7.6.561

Hidayat, R., Firmansyah, A., & Wibowo, S. (2025). Sistem Pelayanan dan Pengelolaan Rekam Medis di Fasilitas Pelayanan Kesehatan Tingkat Pertama. Jurnal Manajemen Kesehatan, 11(3), 201–212.

IBM Security. (2023). Cost of a Data Breach Report 2023. IBM Corporation.

IBM Security. (2024). Cost of a Data Breach Report 2024. IBM Corporation.

Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 22(2), 177–183. https://doi.org/10.1016/j.eij.2020.07.003

Kiani, K., Jameii, S. M., & Rahmani, A. M. (2023). Blockchain-based privacy and security preserving in electronic health: A systematic review. Multimedia Tools and Applications. https://doi.org/10.1007/s11042-023-14488-w

Nowrozy, R., Ahmed, K. E. U., Kayes, A. S. M., & Wang, H. (2024). Privacy preservation of electronic health records in the modern era: A systematic survey. ACM Computing Surveys, 56(8). https://doi.org/10.1145/3653297

Pool, J., Akhlaghpour, S., Fatehi, F., & Burton-Jones, A. (2024). A systematic analysis of failures in protecting personal health data: A scoping review. International Journal of Information Management, 74, 102719. https://doi.org/10.1016/j.ijinfomgt.2023.102719

Tertulino, R., Antunes, N., & Morais, H. (2024). Privacy in electronic health records: A systematic mapping study. Journal of Public Health, 32, 435–454. https://doi.org/10.1007/s10389-022-01795-z