Klinik: Jurnal Ilmiah Kedokteran dan Kesehatan
Volume.5, Nomor.2 Mei 2026
E-ISSN : 2809-2090; P-ISSN : 2809-235X, Hal 353-373
DOI: https://doi.org/10.55606/klinik.v5i2.6465
Tersedia: https://journalcenter.org/index.php/KLINIK

Evaluasi Penggunaan Rekam Medis Elektronik (RME) dalam Peningkatan Keamanan Data Pasien di Puskesmas Haurwangi Kabupaten Cianjur

Yayan Ari Kurniawan[1*], Rian Andriani[2], Yani Restiani Widjaja[3]
[1-3] Universitas Adhirajasa Reswara Sanjaya, Bandung, Indonesia
**Penulis Korespondensi: yayankurniawan.dr@gmail.com*

Abstract. *Digital transformation in the health sector has driven the adoption of Electronic Medical Records (EMR) as an innovative solution to replace manual record-keeping systems traditionally used by healthcare providers. The implementation of EMR in primary healthcare centers plays a strategic role, as it has the potential to improve service efficiency, enhance the quality of patient care, and support data integration across service units. Nevertheless, the adoption of EMR also presents new challenges, particularly related to patient data security and protection. This study aims to evaluate the use of Electronic Medical Records in enhancing patient data security at Haurwangi Public Health Center. The research employed a case study design with a descriptive qualitative approach. Data were collected through observation and in-depth interviews using the GAP Analysis: Status of ISO 27001 Implementation – Checklist instrument. The results indicate that the use of EMR at Haurwangi Public Health Center has supported data integration from patient registration to referral processes and facilitated the preparation of both internal and external reports. However, based on the GAP Analysis referring to the ISO 27001:2022 standard, patient data security requirements have not been fully met, resulting in potential risks of data breaches. Therefore, it is necessary to revise strategic policies in line with current regulations, enhance human resource competencies, implement comprehensive risk management, and conduct regular internal and external audits to strengthen information security based on the principles of Confidentiality, Integrity, and Availability (CIA Triad).*

Keywords: *Data Security; Digital Health Transformation; Electronic Medical Records; ISO 27001:2022; Primary Health Care.*

Abstrak. Transformasi digital di sektor kesehatan mendorong penerapan Rekam Medis Elektronik (RME) sebagai solusi inovatif untuk menggantikan sistem pencatatan manual yang selama ini digunakan oleh penyedia layanan kesehatan. Implementasi RME di Puskesmas memiliki peran strategis karena berpotensi meningkatkan efisiensi pelayanan, kualitas perawatan pasien, serta integrasi data antarunit layanan. Meskipun demikian, penerapan RME juga menimbulkan tantangan baru, khususnya terkait keamanan dan perlindungan data pasien. Penelitian ini bertujuan untuk mengevaluasi penggunaan Rekam Medis Elektronik dalam meningkatkan keamanan data pasien di Puskesmas Haurwangi. Metode penelitian yang digunakan adalah studi kasus dengan pendekatan deskriptif kualitatif. Pengumpulan data dilakukan melalui observasi dan wawancara mendalam dengan menggunakan instrumen *GAP Analysis: Status of ISO 27001 Implementation – Checklist*. Hasil penelitian menunjukkan bahwa penggunaan RME di Puskesmas Haurwangi telah mendukung integrasi data mulai dari proses pendaftaran hingga rujukan, serta mempermudah penyusunan laporan internal dan eksternal. Namun, berdasarkan hasil *GAP Analysis* mengacu pada standar ISO 27001:2022, aspek keamanan data pasien belum sepenuhnya terpenuhi sehingga masih terdapat risiko kebocoran data. Oleh karena itu, diperlukan revisi kebijakan strategis yang selaras dengan regulasi terkini, peningkatan kompetensi sumber daya manusia, penerapan manajemen risiko yang komprehensif, serta pelaksanaan audit internal dan eksternal secara berkala guna memperkuat keamanan informasi berdasarkan prinsip *Confidentiality, Integrity, and Availability* (CIA Triad).

Kata kunci: ISO 27001:2022; Keamanan Data; Puskesmas; Rekam Medis Elektronik; Transformasi Digital Kesehatan.

1. LATAR BELAKANG

Indonesia merupakan salah satu negara berkembang yang terus melakukan pembangunan di berbagai bidang guna mencapai tujuan nasional sebagaimana tercantum dalam Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yaitu melindungi segenap bangsa dan seluruh tumpah darah Indonesia, memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, serta ikut melaksanakan ketertiban dunia berdasarkan kemerdekaan,

Naskah Masuk: 15 Desember 2025; Revisi: 13 Januari 2026; Diterima: 30 Januari 2026;
Tersedia: 02 Februari 2026

perdamaian abadi, dan keadilan sosial. Kesehatan sebagai salah satu unsur kesejahteraan umum harus diwujudkan melalui berbagai upaya kesehatan dalam rangka pembangunan kesehatan yang menyeluruh dan terpadu.

Hak atas pelayanan kesehatan dijamin secara konstitusional sebagaimana diatur dalam Pasal 28 ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan bahwa setiap orang berhak memperoleh pelayanan kesehatan. Selain itu, Pasal 34 ayat (3) menegaskan bahwa negara bertanggung jawab atas penyediaan fasilitas pelayanan kesehatan dan fasilitas pelayanan umum yang layak. Dengan demikian, pelayanan kesehatan menjadi hak asasi setiap warga negara yang wajib dipenuhi oleh negara.

Sebagai sarana pelayanan kesehatan tingkat pertama, Pusat Kesehatan Masyarakat (Puskesmas) memiliki peran strategis dalam penyelenggaraan pelayanan kesehatan. Peraturan Menteri Kesehatan Republik Indonesia Nomor 19 Tahun 2025 tentang Penyelenggaraan Pusat Kesehatan Masyarakat menjelaskan bahwa Puskesmas menyelenggarakan dan mengoordinasikan pelayanan promotif, preventif, kuratif, rehabilitatif, dan/atau paliatif di wilayah kerjanya. Oleh karena itu, Puskesmas dituntut untuk mampu meningkatkan mutu pelayanan melalui pemanfaatan teknologi informasi.

Transformasi digital sektor kesehatan di Indonesia telah menunjukkan manfaat signifikan dalam meningkatkan efisiensi operasional, kualitas layanan, dan aksesibilitas pasien, namun masih menghadapi tantangan seperti keterbatasan konektivitas, resistensi terhadap perubahan, serta keamanan data (Wulandari et al., 2025). Salah satu bentuk nyata dari transformasi digital tersebut adalah penerapan Rekam Medis Elektronik (RME) sebagai solusi inovatif yang menggantikan metode pencatatan manual (Agustiany, 2024). Rekam Medis Elektronik didefinisikan sebagai rekam medis yang dibuat dengan sistem elektronik untuk penyelenggaraan rekam medis dengan prinsip keamanan dan kerahasiaan data (Permenkes, 2022).

Penerapan Rekam Medis Elektronik memiliki peranan penting di Puskesmas karena mampu meningkatkan efisiensi, mempercepat layanan, serta meningkatkan kualitas pelayanan pasien (Wardani, 2022). Institute of Medicine (IOM) menjelaskan bahwa RME mendukung penyimpanan dan pengelolaan data klinis, komunikasi elektronik yang efektif, keselamatan pasien, serta kemudahan administrasi dan pelaporan data (Kusrini et al., 2016). Center of Medicare and Medicaid Services (CMS) juga mendefinisikan RME sebagai catatan medis elektronik yang mencakup data klinis pasien secara komprehensif dan dikelola oleh penyedia layanan kesehatan (Kruse et al., 2017).

Meskipun memiliki berbagai manfaat, penerapan Rekam Medis Elektronik juga menghadirkan ancaman terhadap keamanan dan kerahasiaan data pasien (Musyarofah, 2020). Studi Fifth Annual Benchmark Study tahun 2015 di Amerika Serikat menunjukkan bahwa lebih dari 90% penyedia layanan kesehatan pernah mengalami kebocoran data, bahkan 40% di antaranya mengalami lebih dari lima kali kebocoran dalam dua tahun terakhir (Innab, 2018). Di Indonesia, 70% masyarakat menyatakan kekhawatiran terhadap potensi kebocoran informasi kesehatan (Sari, 2021), yang diperkuat dengan kasus kebocoran 6 juta data medis pasien pada server Kementerian Kesehatan pada tahun 2022 (Sofia, 2022).

Kebocoran data Rekam Medis Elektronik merupakan pelanggaran terhadap prinsip keamanan data pasien yang berdampak pada aspek hukum, etika, dan reputasi institusi kesehatan (Setiawan, 2024). Ketidakamanan data pasien juga berpotensi menimbulkan kerugian material dan non-material serta meningkatkan risiko kejahatan siber (Mulyani et al., 2023). Oleh karena itu, diperlukan penerapan sistem keamanan informasi yang menjamin perlindungan data dari akses yang tidak sah dan penyalahgunaan.

Sebagai respons terhadap meningkatnya risiko pelanggaran data, pemerintah menetapkan berbagai regulasi dan standar keamanan informasi. Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 mewajibkan Rekam Medis Elektronik memenuhi prinsip kerahasiaan, integritas, dan ketersediaan data. Prinsip tersebut sejalan dengan konsep *Confidentiality, Integrity, and Availability* (CIA Triad) (Maya Rani et al., 2024) serta standar ISO/IEC 27001 (Chazar, 2016). Selain itu, prinsip keamanan informasi juga mencakup *privacy, confidentiality, integrity, availability, non-repudiation, authentication,* dan *authorization* (Rahardjo, 2019). Berdasarkan kondisi tersebut serta hasil studi pendahuluan di Puskesmas Haurwangi yang menunjukkan adanya kelemahan pada aspek keamanan data, khususnya pengelolaan akses pengguna, penelitian ini penting dilakukan untuk mengevaluasi penggunaan Rekam Medis Elektronik dalam peningkatan keamanan data pasien di Puskesmas Haurwangi Kabupaten Cianjur.

Berdasarkan latar belakang ini, pentingnya Puskesmas Haurwangi dalam menjaga keamanan data pasien dalam pelaksanaan Rekam Medis Elektronik, serta dampak yang ditimbulkan jika informasi bocor dan berisiko disalahgunakan oleh pihak yang tidak bertanggung jawab. Oleh karena itu peneliti tertarik mengambil judul "Evaluasi Penggunaan Rekam Medis Elektronik Dalam Peningkatan Keamanan Data Pasien di Puskesmas Haurwangi Kabupaten Cianjur".

2. METODE PENELITIAN

Penelitian ini menggunakan desain studi kasus dengan pendekatan deskriptif kualitatif untuk mengevaluasi penerapan Rekam Medis Elektronik (RME) dalam meningkatkan keamanan data pasien di Puskesmas Haurwangi, Kabupaten Cianjur. Penelitian dilaksanakan pada tahun 2024 di Puskesmas Haurwangi yang dipilih karena belum pernah dilakukan evaluasi keamanan data sejak implementasi RME pada Oktober 2023. Penentuan partisipan dilakukan secara purposive sampling, melibatkan Kepala Puskesmas, Penanggung Jawab Klaster 1, Koordinator Sistem Informasi Digital, dan Koordinator Mutu, yang dinilai memiliki pengetahuan dan keterlibatan langsung dalam pengelolaan RME dan sistem keamanan informasi.

Pengumpulan data dilakukan melalui observasi, wawancara mendalam, dan dokumentasi, dengan menggunakan instrumen GAP Analysis: Status of ISO 27001 Implementation–hecklist yang mengacu pada standar ISO/IEC 27001:2022. Evaluasi difokuskan pada aspek keamanan informasi yang meliputi *privacy, integrity, authentication, availability, access control,* dan *non-repudiation*. Data yang diperoleh dianalisis secara kualitatif menggunakan model interaktif Miles dan Huberman, yang mencakup tahap pengumpulan data, reduksi data, penyajian data, serta penarikan dan verifikasi kesimpulan untuk memperoleh gambaran komprehensif mengenai tingkat pemenuhan keamanan data pasien dalam penerapan RME.

3. HASIL DAN PEMBAHASAN

Aspek Keamanan Informasi Rekam Medis Elektronik

Berdasarkan kegiatan observasi dan wawancara yang di lakukkan, maka diperoleh informasi bahwa persentasi pencapaian implementasi aspek keamanan informasi Rekam Medis Elektronik di Puskesmas Haurwangi adalah 47%, dimana hanya 45 (empat puluh lima) dari 93 (sembilan puluh tiga) persyaratan yang terpenuhi. Adapun rinciannya adalah sebagai berikut :

1) Aspek Kerahasiaan (*Confidentiality*)

Menjamin bahwa data Rekam Medis pasien hanya dapat diakses oleh pihak yang memiliki wewenang. Pada aspek kerahasiaan (Privacy) terdapat 13 persyaratan ISO 2700 : 2022

> *"Hasil evaluasi menunjukkan bahwa organisasi telah memenuhi persyaratan utama dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI), khususnya pada aspek konteks organisasi, kepemimpinan, perencanaan, komunikasi, dan operasional. Organisasi telah mengidentifikasi serta melibatkan*

pihak berkepentingan, mempertimbangkan kebutuhan dan ekspektasi mereka, menetapkan sasaran SMKI sesuai persyaratan keamanan informasi, serta mengimplementasikan kontrol yang diperlukan. Selain itu, kebijakan keamanan informasi telah selaras dengan arah strategis organisasi dan dikomunikasikan secara tepat kepada pihak internal maupun eksternal sesuai kebutuhan."

Dari 13 Persyaratan yang ada, 9 persyaratan telah terpenuhi, dengan tingkat pemenuhan sebesar 69%. Pencapaian 69% dalam melindungi kerahasiaan menunjukkan adanya komitmen yang kuat dari Puskesmas Haurwangi dalam melindungi kerahasiaan data pasien.

Keamanan data pasien dilihat dari aspek kerahasiaan sudah lebih baik dibandingkan dengan aspek yang lain. Dimana sebagian besar aktivitas pengoperasian sistem informasi diatur oleh Surat Keputusan Kepala Puskesmas, *Standar Operating Procedure* (SOP), dan panduan pelayanan klinis yang mencakup ketentuan mengenai keamanan data pasien dan termasuk ketentuan kerahasiaan informasi. Akan tetapi di Puskesmas Haurwangi belum melaksanakan audit internal atau eksternal terhadap Sistem Informasi Puskesmas, sehingga belum terdapat pengakuan memenuhi standar keamanan data informasi yang komperhensif.

Aspek kerahasiaan dibuktikan dengan penerapan keamanan data pasien di Puskesmas Haurwangi yakni dengan melakukkan pembatasan akses *log in* di Rekam Medis Elektronik menggunakan *username* dan *passowrd* yang unik, diketahui oleh *user* sebagai pemilik hak ases. Selain itu, akses internet juga dibatasi untuk mencegah akses tidak sah atau penyalahgunaan informasi pasien melalui jaringan internet. Namun, masih dibutuhkan penerapan *log out* secara otomatis, jika tidak ada aktifitas *user* dalam 5 menit. Di samping itu peningkatan kesadaran melalui pelatihan yang lebih intensif bagi petugas dan seluruh karyawan Puskesmas Haurwangi mengenai pentingnya menjaga kerahasiaan informasi pasien. Serta evaluasi dan pemantauan secara rutin terhadap kebijakan yang diterapkan serta langkah-langkah keamanan sangat penting untuk memastikan efektivitas dan kepatuhan dalam perlindungan data pasien.

Penerapan Rekam Medis Elektronik (RME) di Puskesmas membawa berbagai keuntungan dalam meningkatkan efisiensi layanan kesehatan, namun aspek keamanan data pasien khususnya *confidentiality* menjadi tantangan utama yang harus diatasi. Kerahasiaan data pasien mencakup perlindungan terhadap akses tidak sah, kebocoran informasi, dan penyalahgunaan data sensitif yang terkandung di dalam RME.

Sebagaimana diuraikan dalam tinjauan sistematis, implementasi RME harus mempertimbangkan strategi keamanan dan privasi untuk meminimalkan risiko kebocoran data medis yang bersifat sangat pribadi dan berpengaruh pada kepercayaan pasien terhadap sistem layanan kesehatan digital(Puteri et al., 2024).

Pada tingkat operasional di Puskesmas, mekanisme pengendalian akses merupakan salah satu komponen *confidentiality* yang penting. Penelitian di UPT Puskesmas Karangploso menunjukkan bahwa penggunaan autentikasi melalui username dan password untuk masuk ke aplikasi RME membantu menjaga kerahasiaan data dan membatasi akses hanya kepada staf yang berwenang. Mekanisme ini juga dikombinasikan dengan pembatasan hak edit data sehingga hanya pengguna tertentu yang dapat memodifikasi informasi pasien, mengurangi potensi penyalahgunaan atau manipulasi data(Suhariyono et al., 2025).

Menurut Azalia et al., (2024) dalam perspektif etika dan perlindungan hukum, *confidentiality* bukan hanya soal teknologi, tetapi juga kewajiban moral serta kepatuhan terhadap peraturan kesehatan nasional dan standar etika profesi. Prinsip etika dalam penggunaan RME menekankan bahwa tenaga kesehatan memiliki tanggung jawab profesional untuk menjaga kerahasiaan informasi medis pasien dan melindungi hak privasi sebagai bagian dari kualitas pelayanan kesehatan. Tantangan nyata sering muncul dari keterbatasan pelatihan dan pemahaman staf terhadap penggunaan teknologi RME secara aman, sehingga bisa berdampak pada pelanggaran kerahasiaan jika kontrol internal tidak efektif.

Selain kontrol akses dan pelatihan sumber daya manusia, penggunaan teknologi keamanan seperti enkripsi data juga krusial untuk menjaga *confidentiality* RME. Teknik kriptografi, seperti algoritma enkripsi, mampu melindungi data dalam penyimpanan dan selama transmisi, sehingga mengurangi risiko data dapat diakses oleh pihak yang tidak berwenang. Pendekatan ini menjadi penting terutama ketika sistem RME terhubung ke jaringan luas atau berbasis cloud, yang secara teoritis dapat menjadi target serangan siber tanpa langkah proteksi yang memadai(Febriyana & Ichwani, 2024).

Berdasarkan pembahasan diatas dapat disimpulkan bahwa aspek keamanan data pasien dari sisi *confidentiality* dalam penerapan Rekam Medis Elektronik (RME) di Puskesmas Haurwangi telah menunjukkan capaian yang cukup baik dengan tingkat pemenuhan sebesar 69%, yang mencerminkan adanya komitmen institusional dalam melindungi kerahasiaan informasi pasien. Pengaturan akses melalui kebijakan internal, SOP, pembatasan hak akses pengguna, serta penggunaan autentikasi username dan

password telah berkontribusi signifikan dalam mencegah akses tidak sah dan penyalahgunaan data. Namun demikian, belum dilaksanakannya audit keamanan sistem secara internal maupun eksternal menunjukkan bahwa upaya perlindungan kerahasiaan data belum sepenuhnya memenuhi standar keamanan informasi yang komprehensif. Oleh karena itu, diperlukan penguatan sistem melalui penerapan fitur keamanan tambahan seperti *automatic logout*, penggunaan teknologi enkripsi, peningkatan kapasitas sumber daya manusia melalui pelatihan berkelanjutan, serta evaluasi dan pemantauan rutin terhadap kebijakan keamanan. Upaya tersebut penting untuk memastikan keberlanjutan perlindungan kerahasiaan data pasien, meningkatkan kepatuhan terhadap prinsip etika dan regulasi, serta memperkuat kepercayaan masyarakat terhadap layanan kesehatan berbasis digital di Puskesmas.

2) Aspek Integritas (*Integrity)*

Aspek ini menekankan bahwa informasi akurat, lengkap, dan tidak boleh diubah tanpa seijin yang berwenang. Pada aspek Integritas (*Integrity*) terdapat 31 persyaratan ISO 2700 : 2022.

> *"Hasil evaluasi menunjukkan bahwa sebagian besar persyaratan Sistem Manajemen Keamanan Informasi (SMKI) telah terpenuhi, terutama pada aspek konteks organisasi, kepemimpinan, kebijakan, komunikasi, dokumentasi, dan pengendalian operasional. Namun, masih ditemukan ketidaksesuaian pada klausul 4.4 terkait penerapan dan peningkatan berkelanjutan SMKI serta pada klausul 7.5.3(b) terkait perlindungan dokumentasi. Oleh karena itu, diperlukan penguatan mekanisme perbaikan berkelanjutan dan pengendalian dokumen untuk meningkatkan efektivitas SMKI."*

Dari 31 Persyaratan yang ada, 12 persyaratan telah terpenuhi, dengan tingkat pemenuhan sebesar 42%. Pencapaian 42% menunjukkan bahwa keamanan sistem informasi dari aspek integritas belum cukup baik di Puskesmas Haurwangi dalam melindungi data pasien.

Keamanan data pasien di Puskesmas Haurwangi di lihat dari aspek integritas sangat penting bagi *user* untuk memiliki integritas guna memastikan proses entri data dilakukkan dengan baik dan akurat. Aspek integritas pada sistem Rekam Medis Elektronik Puskesmas Haurwangi ditunjukkan saat pengguna melakukkan *log in*. Pengguna diberikan wewenang untuk *log in* menggunakan *username* dan *password* masing-masing.

Puskesmas Haurwangi memiliki prosedur input data yang ketat, dimana penggunaan sistem diwajibkan mengikuti langkah-langkah untuk memastikan data yang dimasukkan akurat dan lengkap. Disamping itu, Rekam Medis Elektronik Puskesmas Haurwangi memiliki kemampuan merekam perubahan yang terjadi atas aksi yang dilakukkan oleh *user*. Dimana jika terjadi kesalahan pada saat penginputan maka dapat dilakukkan perubahan dan data yang dihapus dapat terekam dalam sistem Rekam Medis Elektronik. Akan tetapi jika penghapusan data pasien dan harus menggunakan *code token* atas seizin koordinator Rekam Medis. Segala perubahan data yang terjadi di Rekam Medis Elektronik dapat diketahui. Sistem Rekam Medis Elektronik ini dilengkapi dengan fitur keamanan yang canggih, termasuk enkripsi data dan akses terbatas berdasarkan otorisasi. Hal ini membuktikan bahwa adanya transparansi dan akuntabilitas dalam pengelolaan data Rekam Medis Elektronik.

Integritas sistem Rekam Medis Elektronik terdapat beberapa area yang memerlukan perbaikan. Salah satunya adalah peningkatan ketelitian pengguna terhadap dalam penginputan data untuk itu perlu penguatan pelatihan serta kesadaran staf atau komitmen karyawan terhadap pentingnya integritas data. Serta perlu dilakukan evaluasi manajemen untuk menentukan indikator pengukuran serta audit internal yang terdokumentasi dengan baik berkelanjutan terkait SMKI sehingga Puskesmas Haurwangi tetap dalam koridor kebijakan keamanan informasi

Salah satu komponen penting dalam keamanan data pasien pada penerapan Rekam Medis Elektronik (RME) adalah integritas data, yaitu kemampuan sistem untuk memastikan bahwa informasi pasien tidak mengalami perubahan atau manipulasi yang tidak sah, serta data yang tersimpan tetap akurat dan konsisten sepanjang siklus penggunaannya. Integritas data menjadi krusial karena setiap perubahan yang tidak tercatat atau tidak sah dapat berdampak pada keputusan klinis yang salah dan berujung pada risiko keselamatan pasien. Penelitian yang meninjau keamanan data pada RME menunjukkan bahwa integritas merupakan bagian dari prinsip *CIA Triad* (Confidentiality, Integrity, Availability), di mana sistem harus mampu menjaga keutuhan data dari input hingga penggunaan klinisnya(Setyaningrum & Ricky, 2025).

Di tingkat operasional di fasilitas pelayanan kesehatan primer seperti Puskesmas, penerapan mekanisme kontrol internal untuk menjamin integritas data mencakup pembatasan hak akses pengeditan, rekam *audit log* perubahan data, serta prosedur verifikasi ulang oleh petugas yang berwenang. Penelitian kasus di Puskesmas Jabung menemukan bahwa sistem RME telah menerapkan pembatasan edit data hanya bagi

pengguna dengan hak akses tertentu, dan setiap perubahan tercatat dalam audit log sehingga upaya modifikasi tidak sah dapat terdeteksi. Hal ini menunjukkan bahwa penerapan kontrol akses dan pencatatan perubahan data membantu menjaga integritas informasi pasien dalam sistem RME(Dwi et al., 2023).

Menurut Terry et al., (2019) masih terdapat tantangan dalam pengelolaan integritas data, terutama terkait pelatihan sumber daya manusia dan pemeliharaan sistem yang konsisten. Integritas data tidak hanya bergantung pada teknologi, tetapi juga pada kompetensi dan ketelitian pengguna dalam memasukkan serta memperbarui data pasien. Penelitian pada tingkat internasional menunjukkan bahwa data yang tidak akurat atau tidak lengkap dalam catatan medis elektronik dapat menghambat kepercayaan terhadap sistem serta mengurangi kualitas layanan kesehatan, karena keputusan klinis sangat bergantung pada keakuratan data di RME. Aspek legal dan kebijakan juga berperan dalam menjaga integritas data pasien di RME. Regulasi yang mewajibkan fasilitas kesehatan untuk menerapkan standar keamanan dan tata kelola data memberikan kerangka hukum yang memperkuat tanggung jawab institusi dalam menjaga keutuhan data pasien. Namun, implementasi kebijakan ini perlu diiringi dengan audit berkala dan evaluasi sistem untuk memastikan bahwa mekanisme teknis dan prosedural berjalan sesuai standar yang ditetapkan. Pendekatan kombinasi teknologi (misalnya *version control* dan *checksum*), sumber daya manusia, serta kebijakan internal yang kuat menjadi kunci dalam meningkatkan tingkat integritas data pada RME di Puskesmas(Siregar & Sinaga, 2025)

Berdasarkan pembahasan diatas dapat disimpulkan bahwa keamanan data pasien di Puskesmas Haurwangi dari aspek integritas telah diterapkan dengan cukup baik melalui sistem Rekam Medis Elektronik (RME) yang dilengkapi mekanisme autentikasi pengguna, prosedur input data yang terstandar, pencatatan perubahan data (*audit trail*), serta pembatasan penghapusan data menggunakan otorisasi khusus. Penerapan fitur keamanan seperti enkripsi data dan pengaturan hak akses berbasis kewenangan menunjukkan adanya transparansi dan akuntabilitas dalam pengelolaan informasi medis. Namun demikian, integritas data tidak hanya bergantung pada kecanggihan sistem, tetapi juga pada kompetensi dan ketelitian pengguna dalam melakukan entri dan pembaruan data. Oleh karena itu, diperlukan penguatan pelatihan dan peningkatan kesadaran sumber daya manusia, disertai evaluasi manajemen dan audit internal SMKI yang terdokumentasi dan berkelanjutan, agar integritas data tetap

terjaga dan sistem RME di Puskesmas Haurwangi berjalan sesuai standar keamanan informasi serta mendukung mutu pelayanan kesehatan secara optimal.

3) Aspek Ketersediaan (*Availability*)

Aspek ini menekankan bahwa data atau informasi dan sistem pendukung tersedia saat dibutuhkan. Pada aspek Ketersediaan (*Availability*) terdapat 15 persyaratan ISO 2700 : 2022.

> *"Hasil evaluasi menunjukkan bahwa seluruh persyaratan pada klausul yang ditinjau telah terpenuhi. Organisasi telah menetapkan ruang lingkup SMKI secara jelas, menyediakan sumber daya yang memadai, merencanakan pengelolaan risiko dan peluang, serta memastikan komunikasi informasi keamanan kepada personel internal. Selain itu, dokumentasi SMKI telah tersedia dan layak digunakan sesuai kebutuhan, yang mendukung efektivitas penerapan dan pemeliharaan SMKI."*

Bahwa dari 15 persyaratan yang ada, 6 persyaratan telah terpenuhi, dengan tingkat pemenuhan sebesar 40% . Pencapaian 40% menunjukkan bahwa keamanan sistem informasi dari aspek ketersediaan belum cukup baik di Puskesmas Haurwangi dalam melindungi data pasien.

Aspek ketersediaan informasi kesehatan (availability) dalam penggunaan Rekam Medis Elektronik di Puskesmas Haurwangi saat ini untuk mengoprasikannya masih bersifat hybrid, dimana data pasien dikelola melalui kombinasi antara sistem elektronik dan sistem manual. Dalam sistem hybrid sebagian data pasien diolah dan disimpan secara elektronik, yang memberikan keuntungan dalam efisiensi dan aksesibilitas data. Akan tetapi, masih ada komponen tertentu seperti di Ruang Bersalin/Poned atau RGD (Ruang Gawat Darurat) masih ada data yang dikelola secara manual, yang dapat menjadi kendala dalam mencapai integrasi penuh dan optimalisasi ketersediaan data.

Pada aspek ketersediaan, salah satu tantangan yang dihadapi adalah integrasi data yang dihasilkan oleh Rekam Medis Elektronik dengan pihak eksternal terkait, seperti persetujuan atau penolakan tindakan, Rekam Medis di Pelayanan Obstetri Neonatal Emergensi Dasar (PONED) proses dan klaim non kapitasi asuransi BPJS yang sampai saat ini masih dilakukan secara manual, membuktikan bahwa belum dilakukkan integrasi secara penuh antara sistem Rekam Medis Elektronik dengan pihak eksternal, sehingga dapat mempengaruhi kecepatan dan efisiensi dalam pengelolaan data serta proses administrasi. Namun secara keseluruhan Rekam Medis Elektronik di Puskesmas Haurwangi sudah mendukung aktivitas di semua klaster. *User* dapat mengakses data

pasien dengan mudah dan aman melalui penggunaan *username* dan kata sandi, selama tersedia koneksi internat. Dengan demikian, upaya untuk meningkatkan ketersediaan informasi secara menyeluruh di Puskesmas Haurwangi dapat di fokuskan pada peningkatan integrasi antara sistem Rekam Medis Elektronik dengan pihak eksternal dan meminimalkan pada proses data manual, selain itu harus melakukan audit secara berkala dengan menetapkan indikator pengukuran serta untuk menganalisis dan evalusi risiko keamanan data yang terdokumentasi dengan baik sehingga dapat meningkatkan pelayanan kepada pasien dan memperkuat sistem keamanan informasi di Puskesmas Haurwangi

Aspek ketersediaan (availability) merupakan komponen penting dalam keamanan data pasien pada penerapan Rekam Medis Elektronik (RME), karena menjamin bahwa informasi medis dapat diakses oleh tenaga kesehatan secara tepat waktu dan berkelanjutan saat dibutuhkan dalam pelayanan klinis. Implementasi RME di Puskesmas terbukti meningkatkan ketersediaan data pasien dibandingkan rekam medis manual, karena data tersimpan secara digital dan dapat diakses secara cepat tanpa risiko kehilangan fisik dokumen. Penelitian di UPT Puskesmas Karangploso menunjukkan bahwa RME mampu menyediakan akses data pasien yang lebih responsif dan kontinu, sehingga mendukung efektivitas pelayanan kesehatan dan pengambilan keputusan klinis (Suhariyono et al., 2025). Selain itu, penggunaan sistem penyimpanan terpusat dan mekanisme *backup* turut berperan dalam menjaga ketersediaan data meskipun terjadi gangguan teknis lokal (Dwi et al., 2023).

Ketersediaan data dalam RME sangat dipengaruhi oleh kesiapan infrastruktur teknologi dan manajemen sistem. Keterbatasan jaringan internet, gangguan listrik, serta *downtime* sistem masih menjadi tantangan yang berpotensi menghambat akses data pasien di Puskesmas. Penelitian menunjukkan bahwa tanpa dukungan infrastruktur yang memadai dan pemeliharaan sistem yang berkelanjutan, ketersediaan data dapat terganggu dan berdampak pada kontinuitas pelayanan kesehatan (Setiatin & Azmi, 2024). Oleh karena itu, diperlukan penguatan sistem pendukung seperti jaringan yang stabil, kebijakan *backup* dan pemulihan data, serta dukungan teknis yang berkesinambungan agar aspek ketersediaan RME tetap terjaga dan mampu mendukung keamanan data pasien secara menyeluruh.

4) Aspek Autentikasi (*Authentication)*

Aspek ini memastikan bahwa hanya pengguna yang sah yang dapat mengakses sistem atau data. Pada aspek autentikasi (*Authentication*) terdapat 11 persyaratan ISO 2700 : 2022.

> *"Hasil evaluasi menunjukkan bahwa seluruh persyaratan pada klausul yang ditinjau telah terpenuhi. Organisasi telah menetapkan tanggung jawab keamanan informasi secara jelas, memastikan sasaran SMKI diperbarui sesuai kebutuhan, menentukan batas waktu penyelesaian tindakan, serta mengambil langkah untuk memperoleh dan meningkatkan kompetensi personel yang diperlukan dalam penerapan SMKI."*

Bahwa dari 11 persyaratan yang ada, 4 persyaratan telah terpenuhi, dengan tingkat pemenuhan sebesar 36% . Pencapaian 36% menunjukkan bahwa keamanan sistem informasi dari aspek autentikasi masih terdapat beberapa area yang memerlukan perbaikan di Puskesmas Haurwangi.

Pada aspek autentikasi (*authentication)* di Puskesmas Haurwangi temuan atas ketidaksesuaian dalam sistem Rekam Medis Elektronik biasanya dibahas di dalam rapat internal manajemen. Namun, tidak adanya pencatatan khusus mengenai temuan tersebut membuat proses evaluasi dimasa mendatang menjadi lebih sulit. Akibatnya perbaikan pada aspek autentikasi cenderung dilakukkan secara reaktif, berdasarkan laporan atau pengaduan dari pengguna, dari pada melalui proses evaluasi dan perbaikan rutin yang terstruktur. Meskipun demikian, upaya untuk menjaga keamanan autentikasi di Puskesmas Haurwangi ini telah dilakukan dengan baik oleh tim IT dari pihak eksternal. Salah satu langkah penting yang dilakukan adalah memastikan bahwa setiap pengguna memahami pentingnya menjaga *username* dan *password* dengan catatan tidak memberitahu hal tersebut ke *user* lain, untuk menjaga kerahasiaan informasi dan memastikan bahwa autentifikasi dilakukkan dengan aman oleh seluruh pengguna sistem.

Sosialisasi kepada karyawan sangat perlu dilakukkan melalui saluran lokakarya mini bulanan, apel pagi, termasuk pelatihan langsung dan pembahasan melalui grup WhatsApp, yang bertujuan untuk memastikan bahwa seluruh pengguna memahami dan mematuhi prosedur yang ditetapkan. Langkah ini penting untuk membangun kesadaran di kalangan pengguna mengenai tanggung jawab dalam menjaga keamanan sistem Rekam Medis Elektronik di Puskesmas Haurwangi. Untuk meningkatkan tingkat

kepatuhan efektivitas autentikasi Puskesmas Haurwangi dapat mempertimbangkan penerapan audit internal atau eksternal secara berkelanjutan. Dengan langkah ini Puskesmas Haurwangi ini dapat memperkuat aspek autentikasi dan lebih mendekati standar ISO 27001 yang pada akhirnya akan meningkatkan keseluruhan keamanan informasi di Puskesmas Haurwangi

Aspek autentikasi merupakan elemen fundamental dalam keamanan Rekam Medis Elektronik (RME) karena memastikan bahwa hanya pengguna yang sah dan berwenang yang dapat mengakses serta mengelola data pasien. Autentikasi yang efektif berperan mencegah akses tidak sah, penyalahgunaan informasi, dan pelanggaran privasi, sehingga menjaga kepercayaan pasien terhadap layanan kesehatan digital di Puskesmas. Penerapan autentikasi melalui kredensial unik seperti *username* dan *password*, serta pembatasan akses berdasarkan peran (*role-based access control*), terbukti mampu membedakan kewenangan antara petugas klinis, pendaftaran, dan administrasi(Rohman et al., 2025). Studi di Klinik Assalammedicare menunjukkan bahwa mekanisme autentikasi ini secara signifikan membatasi akses hanya kepada petugas berwenang dan meningkatkan perlindungan data pasien dari ancaman internal maupun eksternal (Ikhtiar et al., 2023;Zahirah et al., 2025).

Selain sebagai verifikasi identitas, autentikasi pada RME terintegrasi dengan kontrol akses dan *audit log* untuk memastikan setiap aktivitas pengguna dapat ditelusuri secara akuntabel. Autentikasi yang kuat, jika dikombinasikan dengan pengendalian hak akses dan pemantauan aktivitas, terbukti menurunkan risiko pelanggaran data akibat penyalahgunaan kredensial (Asih et al., 2024). Namun demikian, tantangan implementasi masih mencakup kebutuhan pembaruan mekanisme keamanan dan peningkatan kapasitas sumber daya manusia. Oleh karena itu, penguatan pelatihan pengguna, penerapan autentikasi multifaktor (*multi-factor authentication/MFA*), serta evaluasi berkala terhadap kebijakan autentikasi menjadi langkah strategis untuk meningkatkan keamanan data pasien secara berkelanjutan di Puskesmas.

5) Aspek Kontrol Akses (*Access Control)*

Aspek ini mengatur dan membatasi akses ke sistem data atau informasi berdasarkan peran dan kebutuhan kerja. Pada aspek kontrol akses (Access Control) terdapat 17 persyaratan ISO 2700 : 2022.

> *"Hasil evaluasi menunjukkan bahwa seluruh persyaratan pada klausul yang ditinjau telah terpenuhi. Organisasi telah mempertimbangkan keterkaitan dan ketergantungan dengan pihak ketiga, mengintegrasikan persyaratan SMKI ke*

dalam proses bisnis, serta menetapkan kebijakan yang mencakup komitmen terhadap pemenuhan persyaratan dan perbaikan berkelanjutan. Selain itu, tanggung jawab dan wewenang keamanan informasi telah ditetapkan dan dikomunikasikan, kebutuhan sumber daya dan kompetensi personel telah ditentukan, mekanisme komunikasi informasi keamanan telah diatur dengan jelas, pengendalian dokumentasi telah diterapkan secara menyeluruh, serta kriteria operasional dan penanggung jawab pemantauan kinerja SMKI telah ditetapkan."

Bahwa dari 17 persyaratan yang ada, 10 persyaratan telah terpenuhi, dengan tingkat pemenuhan sebesar 59% . Pencapaian 59% menunjukkan bahwa keamanan sistem informasi dari aspek kontrol akses sebagian besar sudah dipenuhi di Puskesmas Haurwangi, sehingga masih terdapat ruang untuk peningkatan dalam melindungi data pasien.

Kontrol akses Rekam Medis Elektronik di Puskesmas Haurwangi diterapkan melalui penentuan hak istimewa pengguna, yang secara spesifik mengatur apa yang dapat diakses oleh setiap pengguna dalam pengoperasian sistem informasi. Pembatasan akses ini bertujuan untuk menjaga kerahasiaan dan privasi pasien, serta mencegah modifikasi yang tidak sah terhadap data Rekam Medis. Dengan demikian, hanya individu yang memiliki otorisasi yang tepat yang dapat mengakses, mengubah, atau memperbarui informasi sensitif, yang merupakan prinsip dasar dalam menjaga keamanan informasi.

Lebih lanjut, setiap dokter yang melakukan pencatatan data medis pasien di Puskesmas Haurwangi memiliki hak akses khusus untuk mengedit catatan medis. Pendekatan ini memastikan bahwa informasi pasien hanya diakses dan dikelola oleh profesional medis yang secara langsung bertanggung jawab atas perawatan mereka, sehingga meningkatkan perlindungan terhadap kerahasiaan dan integritas data medis.

Pengaturan ini juga berfungsi sebagai langkah pencegahan terhadap potensi pelanggaran privasi dan menjamin bahwa hanya pihak yang berwenang dan relevan yang dapat mengakses data medis pasien. Namun, untuk mencapai kepatuhan yang lebih tinggi terhadap standar keamanan data pasien, Puskesmas Haurwangi dapat mempertimbangkan untuk memperkuat kebijakan dan prosedur kontrol aksesnya. Ini dapat mencakup peninjauan berkala terhadap hak akses pengguna, pelaksanaan identifikasi dan tata kelola risiko keamanan data yang terdokumentasi dan audit

internal untuk memastikan bahwa hak akses yang diberikan masih sesuai dengan peran dan tanggung jawab pengguna, serta meningkatkan pelatihan dan sosialisasi terkait pentingnya kontrol akses di kalangan karyawan untuk memperkuat perlindungan terhadap data pasien, sehingga akan berkontribusi pada peningkatan kualitas layanan kesehatan yang diberikan.

Aspek kontrol akses merupakan elemen krusial dalam sistem keamanan Rekam Medis Elektronik (RME) karena berfungsi mengatur dan membatasi hak pengguna dalam mengakses data pasien sesuai dengan peran dan tanggung jawabnya. Penerapan kontrol akses berbasis peran (*role-based access control/RBAC*) memastikan bahwa petugas pendaftaran, tenaga kesehatan, dan staf administrasi hanya dapat mengakses informasi yang relevan dengan tugasnya, sehingga mengurangi risiko kebocoran dan penyalahgunaan data medis. Studi tentang keamanan sistem RME menunjukkan bahwa pengelolaan hak akses yang jelas dan terstruktur dapat meningkatkan perlindungan data pasien serta mendukung kepatuhan terhadap prinsip kerahasiaan dan keamanan informasi kesehatan (Wardani et al., 2024).

Selain pembatasan hak akses, kontrol akses yang efektif pada RME juga terintegrasi dengan *audit trail* untuk mencatat seluruh aktivitas pengguna dalam sistem. Integrasi ini memungkinkan fasilitas pelayanan kesehatan, termasuk Puskesmas, untuk melakukan penelusuran aktivitas jika terjadi insiden keamanan serta meningkatkan akuntabilitas pengguna. Tinjauan sistematis terhadap kontrol akses dalam sistem rekam medis elektronik menunjukkan bahwa kombinasi antara mekanisme otorisasi yang tepat dan pencatatan aktivitas sistem secara konsisten mampu meningkatkan keamanan data pasien secara signifikan tanpa menghambat proses pelayanan kesehatan(Cobrado et al., 2024).

Penerapan kontrol akses pada sistem Rekam Medis Elektronik (RME) di Puskesmas Haurwangi telah dilaksanakan dengan cukup baik melalui pengaturan hak akses berbasis peran yang membatasi akses pengguna sesuai dengan tugas dan tanggung jawabnya, khususnya pemberian kewenangan khusus kepada tenaga medis dalam pengelolaan data klinis pasien. Mekanisme ini berkontribusi dalam menjaga kerahasiaan, privasi, dan integritas data pasien serta meningkatkan akuntabilitas melalui pencatatan aktivitas pengguna dalam sistem. Meskipun demikian, optimalisasi keamanan data masih memerlukan penguatan kebijakan dan prosedur kontrol akses secara berkelanjutan, antara lain melalui peninjauan hak akses secara berkala, audit internal yang terdokumentasi, serta peningkatan pelatihan dan kesadaran seluruh

karyawan terhadap pentingnya kontrol akses. Upaya tersebut diharapkan dapat memperkuat tata kelola keamanan informasi kesehatan dan mendukung peningkatan kualitas pelayanan kesehatan di Puskesmas Haurwangi

6) Aspek Nir-sangkal (*Non-Repudiation)*

Aspek ini memastikan bahwa seseorang tidak bisa menyangkal telah melakukkan tindakan terkait data/informasi. Pada aspek Nir-sangkal (*Non-Repudiation*) terdapat 8 persyaratan ISO 2700 : 2022.

> *"Hasil evaluasi menunjukkan bahwa seluruh persyaratan pada klausul yang ditinjau telah terpenuhi. Manajemen telah mendukung peran kepemimpinan dalam keamanan informasi, kebijakan keamanan informasi telah dipahami di seluruh organisasi, sasaran SMKI dapat dikomunikasikan secara efektif, serta organisasi telah memiliki mekanisme penanganan insiden keamanan informasi yang sesuai dengan tingkat dampaknya."*

Bahwa dari 8 persyaratan yang ada, 4 persyaratan telah terpenuhi, dengan tingkat pemenuhan sebesar 50%. Pencapaian 50% menunjukkan bahwa keamanan sistem informasi dari aspek Nir-sangkal sebagian besar sudah dipenuhi di Puskesmas Haurwangi, tetapi masih perlu meningkatkan pemenuhan persyaratan untuk melindungi data pasien

Aspek nir-sangkal pada Rekam Medis Elektronik di Puskesmas Haurwangi diimplementasikan melalui kemampuan sistem dalam mencatat setiap jejak perubahan data, baik berupa penambahan maupun modifikasi yang dilakukan oleh pengguna. Setiap aktivitas yang terjadi dalam sistem secara otomatis direkam dan disimpan, sehingga tidak ada perubahan yang bisa dimanipulasi atau dihapus tanpa tercatat. Catatan ini berfungsi sebagai bukti audit dan hanya dapat diakses oleh tim IT dari pihak ketiga yang berwenang, yang bertanggung jawab untuk memantau dan menjaga integritas data.

Penerapan mekanisme *nir-sangkal* ini tidak hanya berfungsi sebagai perlindungan terhadap integritas data, tetapi juga meningkatkan akuntabilitas setiap pengguna sistem. Setiap tindakan, termasuk akses, perubahan, atau penghapusan data, dapat dilacak secara rinci, memastikan bahwa semua aktivitas tercatat dengan baik dan dapat ditinjau jika diperlukan. Hal ini sangat penting dalam konteks layanan kesehatan, di mana akurasi dan keandalan data merupakan faktor krusial untuk keselamatan pasien dan pengambilan keputusan medis.

Oleh karena itu, dengan adanya mekanisme nir-sangkal ini Rekam Medis Elektronik di Puskesmas Haurwangi mampu memberikan perlindungan yang lebih tinggi

terhadap data pasien, memastikan bahwa setiap perubahan yang dilakukan dapat dipertanggung jawabkan. Selain itu, perlu meningkatkan standarisasi aspek nir-sangkal keamanan data pasien dengan melakukan audit internal secara berkala sehingga dapat menjaga keamanan data pasien di Puskesmas Haurwangi.

Meningkatkan Keamanan Data Paien dalam Penggunaan Rekam Medis Elektronik

Keamanan data dan informasi merupakan serangkaian upaya sistematis untuk melindungi data dari akses, gangguan, penyalahgunaan, penggunaan, maupun modifikasi yang tidak sah (Zen et al., 2023). Dalam konteks pelayanan kesehatan, data dan informasi pasien merupakan aset yang sangat bernilai karena berkaitan langsung dengan aspek klinis, hukum, dan etika pelayanan. Oleh karena itu, Puskesmas Haurwangi perlu menerapkan langkah-langkah keamanan data yang komprehensif guna mencegah potensi ancaman yang dapat menyebabkan kebocoran, kerusakan, atau kehilangan data pasien, khususnya dalam pemanfaatan Rekam Medis Elektronik (RME).

Hasil GAP Analysis berdasarkan standar ISO 27001:2022 menunjukkan bahwa masih terdapat 47% dari 93 klausa persyaratan yang belum terpenuhi secara optimal di Puskesmas Haurwangi. Temuan ini mengindikasikan perlunya prioritas perbaikan dalam pengelolaan keamanan informasi, antara lain melalui revisi kebijakan agar selaras dengan regulasi perlindungan data terbaru, penguatan kompetensi sumber daya manusia terkait keamanan informasi RME, implementasi manajemen risiko yang terstruktur, serta pelaksanaan audit internal secara berkelanjutan dan audit eksternal berstandar internasional. Upaya perbaikan tersebut diharapkan mampu memperkuat penerapan prinsip CIA Triad, yaitu Confidentiality, Integrity, dan Availability, sebagai fondasi utama dalam keamanan data pasien (Hermawan et al., 2022).

Seiring meningkatnya digitalisasi layanan kesehatan, keamanan data pasien dalam Electronic Medical Record (EMR) menjadi isu yang semakin krusial akibat tingginya risiko pelanggaran data dan akses tidak sah terhadap informasi medis yang bersifat sensitif. Berbagai pendekatan teknologi dan manajerial telah dikembangkan untuk meningkatkan perlindungan data pasien, dengan tujuan menjaga kerahasiaan, integritas, dan ketersediaan data, serta meningkatkan kepercayaan pengguna terhadap sistem informasi kesehatan. Pendekatan ini menuntut integrasi antara kebijakan organisasi, tata kelola keamanan, serta pemanfaatan teknologi keamanan yang andal.

Salah satu teknologi yang berpotensi meningkatkan keamanan EMR adalah blockchain, yang menawarkan mekanisme penyimpanan data terdesentralisasi dan bersifat immutable,

sehingga sulit dimanipulasi tanpa otorisasi. Integritas data dijaga melalui teknik hashing kriptografis yang kuat, seperti algoritma SHA-256, yang memungkinkan pendeteksian perubahan data secara real time (El-Hamed et al., 2023). Selain itu, blockchain memberikan peluang peningkatan kontrol pasien terhadap data medisnya, di mana pasien dapat mengatur hak akses dan berbagi data secara aman dengan penyedia layanan kesehatan melalui sistem penyimpanan terdesentralisasi (Smitha et al., 2024).

Selain pemanfaatan blockchain, teknik enkripsi merupakan komponen fundamental dalam pengamanan EMR. Penggunaan Advanced Encryption Standard (AES) terbukti efektif dalam melindungi data medis pasien baik saat penyimpanan maupun transmisi, sehingga informasi sensitif tidak dapat diakses oleh pihak yang tidak berwenang. Penerapan autentikasi berlapis, seperti One-Time Passwords (OTP), juga mampu memperkuat proses verifikasi identitas pengguna dan meminimalkan risiko penyalahgunaan kredensial akses ke sistem EMR (Ononiwu, 2024).

Upaya peningkatan keamanan EMR perlu dilengkapi dengan penilaian kerentanan sistem secara berkala. Pengujian penetrasi (penetration testing) menjadi metode penting untuk mengidentifikasi celah keamanan, seperti SQL Injection dan Cross-Site Scripting (XSS), yang berpotensi dimanfaatkan oleh pihak tidak bertanggung jawab. Selain itu, pembaruan sistem dan penerapan patch keamanan secara rutin, termasuk pada infrastruktur jaringan, sangat diperlukan untuk mengurangi risiko eksploitasi terhadap kerentanan yang telah diketahui (Putrawansyah & Sutabri, 2024). Pendekatan komprehensif yang mengombinasikan teknologi, evaluasi sistem, dan tata kelola keamanan yang kuat menjadi kunci dalam menjaga keamanan data pasien pada sistem EMR secara berkelanjutan di Puskesmas.

4. KESIMPULAN DAN SARAN

Penerapan Rekam Medis Elektronik (RME) di Puskesmas Haurwangi terbukti meningkatkan efisiensi pelayanan, mempercepat proses layanan kesehatan, serta mendukung integrasi data mulai dari pendaftaran hingga rujukan dan pelaporan internal maupun eksternal, meskipun implementasinya masih bersifat hybrid dan audit mutu belum dilaksanakan secara optimal. Hasil evaluasi keamanan data pasien berdasarkan *GAP Analysis* mengacu pada standar ISO 27001:2022 menunjukkan bahwa pemenuhan aspek keamanan informasi, khususnya integritas, ketersediaan, dan autentikasi, masih belum optimal sehingga berpotensi menimbulkan risiko kebocoran data pasien. Oleh karena itu, peningkatan keamanan data memerlukan revisi kebijakan strategis yang selaras dengan regulasi terkini, penguatan kompetensi sumber daya manusia, penerapan manajemen risiko yang komprehensif, serta

pelaksanaan audit internal dan eksternal secara berkelanjutan guna memperkuat prinsip *Confidentiality, Integrity, and Availability* (CIA Triad) dalam pengelolaan Rekam Medis Elektronik.

DAFTAR REFERENSI

Abd El-Hamed, O. M., Abd El-Samie, F. E., Abd El-Atty, S. M., Hemdan, E. E.-D., & Badawy, W. (2023). Enhancement of electronic medical record (EMR) security in private networks with blockchains. *Proceedings of the IEEE International Conference on Engineering and Emerging Multidisciplinary*, 1–8. https://doi.org/10.1109/ICEEM58740.2023.10319566

Abdussamad, Z. (2021). *Metode penelitian kualitatif*. CV Syakir Media Press. https://doi.org/10.31219/osf.io/juwxn

Adafiah, M., Rohendi, A., & Andriani, R. (2023). Pengaruh pelayanan satuan darurat terhadap kepuasan pasien selama pandemi Covid-19 di Rumah Sakit Muhammadiyah Bandung. *Jurnal Manajemen Rumah Sakit, 1*(1), 23–41. https://doi.org/10.36080/jem.v13i1.2854

Adil, A., et al. (2023). *Metode penelitian kuantitatif, kualitatif: Teori dan praktik*. Get Press Indonesia.

Agustiany, I., Andriani, R., & Suwardhani, A. D. (2024). Efektivitas kualitas rekam medis elektronik dalam meningkatkan produktivitas dan manajemen keselamatan pasien: Studi kualitatif di RSIA Mutiara Putri Bandar Lampung. *Intisari Sains Medis, 15*(3), 1061–1064. https://doi.org/10.15562/ism.v15i3.2158

Asih, H. A., et al. (2024). Evaluasi keamanan data pasien pada rekam medis elektronik dengan systematic literature review. *Jurnal Ilmiah FIFO, 16*(2), 104–110. https://doi.org/10.22441/fifo.2024.v16i2.001

Azalia, Z., Ramadhaningrum, O., Nuranisa, S. S., Alya, P., & Kurnaesih, E. (2024). Penerapan prinsip etika pada penggunaan rekam medis elektronik. *Jurnal Kesmas Untika Luwuk: Public Health Journal, 15*, 1–10. https://doi.org/10.51888/phj.v15i2.284

Chazar, C., & Ramdhani, M. A. (2016). Model perencanaan keamanan sistem informasi menggunakan metode OCTAVE dan ISO 27001:2005. *Seminar Nasional Telekomunikasi dan Informatika*.

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

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage Publications.

Departemen Kesehatan Republik Indonesia. (2006). *Pedoman penyelenggaraan dan prosedur rekam medis rumah sakit di Indonesia*. Direktorat Jenderal Pelayanan Medik.

Dwi, L., Prabawati, M., Ikawati, F. R., & Afifah, L. (2023). Tinjauan keamanan data rekam medis elektronik di Puskesmas Jabung. *Jurnal Vokasi, 4*(2), 87–94.

Febriyana, V., & Ichwani, A. (2024). Keamanan data rekam medis elektronik menggunakan teknik kriptografi: Literature review. *Jurnal Komputasi, 12*(2), 165–175. https://doi.org/10.23960/komputasi.v12i2.276

Hermawan, A., Hartati, T., & Wijaya, Y. A. (2022). Analisis keamanan data melalui website Zahra Software menggunakan metode CIA triad. *Jurnal Pengembangan IT, 7*(3), 125–130. https://doi.org/10.30591/jpit.v7i3.3428

Ikhtiar, R. W., Hendry, Z., & Hidayat, R. (2023). Hubungan budaya kerja dengan kelengkapan data pelayanan pasien pada SIMKES Puskesmas Wajageseng. *Jurnal Kesehatan Tropis Indonesia, 1*(4), 1–6. https://doi.org/10.63265/jkti.v1i4.81

Innab, N. (2018). Availability, accessibility, privacy and safety issues facing electronic medical records. *International Journal of Security, Privacy and Trust Management, 7*(1), 1–10. https://doi.org/10.5121/ijsptm.2018.7101

ISO/IEC. (2022). *ISO/IEC 27001:2022 information security management systems*. ISO.

Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. *Journal of Medical Systems, 41*(8), 127. https://doi.org/10.1007/s10916-017-0778-4

Musyarofah, R. S., & Bisma, R. A. (2020). Pembuatan SOP keamanan informasi berdasarkan ISO/IEC 27001 dan 27002. *Journal of Emerging Information Systems and Business Intelligence, 1*(1), 43–50.

Ononiwu, C. C., & Mgbeafulike, I. J. (2024). Maintaining integrity and confidentiality of patients' records using an enhanced security technique. *International Journal of Innovative Science and Research Technology*, 1767–1773. https://doi.org/10.38124/ijisrt/IJISRT24OCT1787

Peraturan Menteri Kesehatan Republik Indonesia Nomor 19 Tahun 2015 tentang Pusat Kesehatan Masyarakat.

Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis.

Puteri, D., Pramesti, A., Ayuningtyas, D., & Verdi, R. (2024). Keamanan dan kerahasiaan data medis pasien dalam implementasi rekam medis elektronik. *PREPOTIF: Jurnal Kesehatan Masyarakat, 8*, 7691–7702. https://doi.org/10.31004/prepotif.v8i3.38445

Putrawansyah, A., & Sutabri, T. (2024). Analisis keamanan aplikasi rekam medis elektronik menggunakan penetration testing. *Router: Jurnal Teknik Informatika dan Terapan, 2*(4). https://doi.org/10.62951/router.v2i4.268

Raharjo, B. (2019). *Keamanan sistem informasi*. Yayasan Prima Agus Teknik.

Rohman, H., Lauma, A. S., Pambudi, S. D., & Narendra, I. (2025). Evaluation of core security principles in electronic medical records. *Procedia of Engineering and Life Science, 9*, 43–51.

Setiatin, S., & Azmi, A. R. (2024). Analysis of patient data security aspects in EMR implementation at Hospital X Bandung. *International Journal Prima Husada Health, 1*(2), 173–180.

Setyaningrum, E., & Ricky, A. V. (2025). Analisis keamanan data pasien berdasarkan CIA triad di RSUD X Jawa Tengah. *Jurnal Ners, 9*, 4216–4221. https://doi.org/10.31004/jn.v9i3.46352

Siregar, R. A., & Sinaga, H. S. R. (2025). Aspek hukum perlindungan data pasien dalam penyelenggaraan RME di Indonesia. *Jurnal Hukum To-Ra, 11*(1), 106–116. https://doi.org/10.55809/tora.v11i1.433

Smitha, G. V., Ghorpade, A., Asthik, K., & Yadav, N. (2024). CryptoRecord: Advancing EMR security with blockchain technology. *Proceedings of the ICOICI*, 83–89. https://doi.org/10.1109/ICOICI62503.2024.10696021

Suhariyono, U. S., Ikawati, F. R., & Afifah, N. (2025). Analisis aspek keamanan informasi data pasien pada RME di UPT Puskesmas Karangploso. *Jurnal Manajemen Informasi Kesehatan Indonesia, 13*(1).

Terry, A. L., et al. (2019). A basic model for assessing primary health care EMR data quality. *BMC Medical Informatics and Decision Making, 19*(1), 30. https://doi.org/10.1186/s12911-019-0740-0

Wardani, E., Putra, D. H., Sonia, D., & Yulia, N. (2024). Keamanan sistem informasi RME di RS Islam Jakarta Sukapura. *RAMMIK, 3*(2), 31–38.

Zahirah, I., Putry, A. D., Cahyani, N., Della, A. R., & Dewi, A. P. (2025). Analisis keamanan autentikasi pengguna pada RME di Klinik Assalammedicare. *Jurnal Rekam Medis dan Informasi Kesehatan, 4*(2), 57–65.