Jurnal Manajemen Dan Administrasi Rumah Sakit (MARSI)
Vol. 10 No 4, Oktober 2026
https://ejournal.urindo.ac.id/index.php/MARSI
E-ISSN: 2865-6583
P-ISSN: 2868-6298
10.52643/marsi.v10i4.9111

ANALISIS PENERAPAN KEAMANAN DATA PADA SISTEM REKAM MEDIS ELEKTRONIK BERDASARKAN PRINSIP CIA DI PUSKESMAS CEMPAKA PUTIH KOTA BANJARMASIN

ANALYSIS OF DATA SECURITY IMPLEMENTATION IN ELECTRONIC MEDICAL RECORD SYSTEMS BASED ON CIA TRIAD PRINCIPLES AT CEMPAKA PUTIH PUBLIC HEALTH CENTER, BANJARMASIN CITY

Ahmad Rifa'i[1], Dwi Iskandar[2]
[1]Program Studi Manajemen Informasi Kesehatan, Politeknik Indonusa Surakarta
[2]Program Studi Teknologi Rekayasa Perangkat Lunak, Politeknik Indonusa Surakarta
Email : 25.ahmad.rifai@poltekindonusa.ac.id

ABSTRAK

Penggunaan Rekam Medis Elektronik (EMR) di lembaga kesehatan menawarkan beberapa keuntungan dalam meningkatkan efisiensi dan kualitas layanan, meskipun juga menimbulkan masalah terkait keamanan data pasien. Studi ini bertujuan untuk mengevaluasi penggunaan keamanan data di dalam sistem Rekam Medis Elektronik, berdasarkan prinsip Triad CIA: kerahasiaan, integritas, dan ketersediaan, di Puskesmas Cempaka Putih, Kota Banjarmasin. Penelitian ini menggunakan metodologi deskriptif dengan pendekatan kualitatif. Informan penelitian meliputi petugas rekam medis, petugas registrasi, dan tenaga kesehatan yang terlibat dalam penggunaan sistem EMR. Pengumpulan data dilakukan melalui wawancara komprehensif, observasi langsung sistem rekam medis elektronik, dan pemeriksaan dokumen yang berkaitan dengan aturan dan prosedur keamanan data. Analisis data tematik dilakukan berdasarkan tiga elemen utama Triad CIA. Temuan studi menunjukkan bahwa kerahasiaan telah dijaga melalui implementasi nama pengguna, kata sandi, dan pembatasan akses pengguna; namun, masalah tetap ada dengan akun bersama, tidak adanya fitur logout otomatis, dan kurangnya kebijakan keamanan data yang komprehensif. Sistem telah menetapkan mekanisme perbaikan data sesuai dengan peraturan; Meskipun demikian, fitur jejak audit masih belum memadai dan gagal menangkap aktivitas pengguna secara komprehensif. Ketersediaan sistem dipastikan oleh jaringan internet cadangan, sumber daya listrik alternatif, dan kolaborasi dengan pemasok aplikasi. Namun, saat ini sistem tersebut masih kekurangan Prosedur Operasi Standar (SOP) yang terdefinisi untuk mengelola waktu henti. Studi ini menunjukkan bahwa efektivitas keamanan data RME dipengaruhi oleh gabungan variabel teknologi, tata kelola organisasi, dan perilaku pengguna. Temuan penelitian dapat memberikan dasar untuk menilai dan meningkatkan kebijakan keamanan informasi, kontrol akses, pengembangan jejak audit, dan kesiapan keberlanjutan layanan dalam penerapan RME di lembaga perawatan kesehatan primer.

Kata kunci: *Availability***,** CIA TRIAD*, Confidentiality, Integrity,* Keamanan Data, Rekam Medis Elektronik

ABSTRACT

The use of Electronic Medical Records (EMR) in healthcare institutions offers several advantages in enhancing efficiency and service quality, although it also presents issues with patient data security. This study seeks to evaluate the use of data security within the Electronic Medical Records system, grounded in the principles of the CIA Triad: confidentiality, integrity, and availability, at the Cempaka Putih Community Health Center in Banjarmasin City. The research employed a descriptive methodology using a qualitative approach. The research informants included medical records officers, registration officers, and health professionals involved in the utilization of the EMR system. Data collection was executed via comprehensive interviews, direct observation of the electronic medical record system, and examination of

documentation pertaining to data security rules and procedures. Thematic data analysis was performed based on the three primary elements of the CIA Triad. The study's findings demonstrate that confidentiality has been upheld through the implementation of usernames, passwords, and user access restrictions; however, issues persist with shared accounts, the absence of an automatic logout feature, and a lack of a comprehensive data security policy. The system has established a data repair mechanism in accordance with regulations; However, the audit trail feature remains inadequate and fails to capture user activities comprehensively. The system's availability is ensured by a backup internet network, alternate power sources, and collaboration with application suppliers. Nonetheless, it currently lacks a defined Standard Operating Procedure (SOP) for managing downtime. This study demonstrates that the efficacy of RME data security is affected by a confluence of technological variables, organizational governance, and user behavior. The research findings can provide a foundation for assessing and enhancing information security policies, access control, audit trail development, and service continuity readiness in the adoption of RME at primary healthcare institutions.

Keywords: Availability, CIA Triad, Confidentiality, Electronic Medical Record, Data Security, Integrity.

PENDAHULUAN

Beberapa tahun terakhir telah menyaksikan kemajuan substansial dalam teknologi digital di industri kesehatan (Cholik, 2021). Kemajuan dalam teknologi informasi telah memfasilitasi penggunaan internet secara luas di berbagai sektor industri dan upaya masyarakat (Anggraeni dkk., 2022). Salah satu metode pelaksanaannya dalam layanan kesehatan adalah penggunaan Rekam Medis Elektronik (EMR). Sistem ini beroperasi untuk memelihara informasi pasien secara komprehensif, meliputi data identitas, riwayat pemeriksaan, hasil diagnostik, prosedur medis yang diberikan, dan terapi atau perawatan yang dilakukan oleh tenaga kesehatan. Penggunaan EMR dianggap berhasil dalam meningkatkan layanan kesehatan, mempercepat perolehan informasi pasien, mengurangi ketergantungan pada dokumentasi kertas, dan memfasilitasi kesinambungan perawatan (Gede dkk., 2024). Di Indonesia, kebijakan pemerintah mengenai implementasi Rekam Medis Elektronik, sebagaimana diuraikan dalam Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis, semakin memperkuat inisiatif transformasi digital di sektor kesehatan. Peraturan ini mewajibkan semua lembaga layanan kesehatan, termasuk klinik kesehatan masyarakat, untuk mengadopsi rekam medis elektronik (Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis).

Walaupun menawarkan berbagai keuntungan, implementasi RME juga menghadirkan tantangan yang berkaitan dengan perlindungan data dan informasi kesehatan pasien. Rekam medis termasuk kategori data yang bersifat rahasia dan sensitif sehingga rentan terhadap berbagai risiko, seperti kebocoran informasi, penyalahgunaan hak akses, perubahan data tanpa kewenangan, maupun terganggunya ketersediaan sistem. Ancaman terhadap keamanan tersebut dapat bersumber dari aspek teknis, misalnya serangan siber dan kegagalan sistem, Baik faktor teknologi maupun non-teknis, termasuk penggunaan akun bersama, langkah-langkah pengendalian akses yang tidak memadai, dan kurangnya pengetahuan pengguna

tentang pentingnya keamanan informasi. Oleh karena itu, keamanan data merupakan faktor penting yang perlu dipertimbangkan saat menerapkan sistem EMR di lembaga perawatan kesehatan (Kruse et al., 2017).

Berbagai organisasi kesehatan internasional menegaskan bahwa implementasi digitalisasi dalam pelayanan kesehatan perlu disertai dengan penguatan aspek keamanan informasi, mengingat data kesehatan merupakan jenis data sensitif yang memiliki tingkat kerentanan tinggi terhadap kebocoran, perubahan data tanpa otorisasi, maupun kehilangan informasi (Thapa & Camtepe, 2021). Peningkatan penggunaan teknologi berbasis internet, *cloud computing*, dan *Internet of Medical Things* (IoMT) turut berkontribusi terhadap meningkatnya ancaman keamanan siber pada sistem kesehatan di berbagai negara (Ghubaish et al., 2021). Ancaman tersebut meliputi pencurian identitas pasien, serangan *ransomware*, akses tanpa hak, serta pemanfaatan data kesehatan oleh pihak yang tidak memiliki kewenangan (Kagita et al., 2022). Lebih lanjut, penelitian yang dilakukan oleh Isabel Herrera Montano dkk. menunjukkan bahwa ancaman yang timbul dari lingkungan internal organisasi merupakan risiko utama dalam sistem informasi kesehatan, karena sifat sensitif data pasien memfasilitasi penyalahgunaan hak akses oleh pengguna internal (Herrera Montano dkk., 2026). Situasi tersebut tidak hanya berpotensi menimbulkan kerugian bagi fasilitas pelayanan kesehatan, tetapi juga dapat mengancam keamanan dan privasi pasien sebagai pemilik data medis yang bersangkutan (Tedjasukmana & Riswadi, 2021).

Secara global, penilaian keamanan data dalam Rekam Medis Elektronik (EMR) biasanya sesuai dengan Triad CIA, yang meliputi kerahasiaan, integritas, dan ketersediaan. Triad CIA adalah konsep keamanan siber terkemuka yang menekankan kerahasiaan, integritas, dan ketersediaan sebagai tiga elemen penting yang diperlukan untuk perlindungan data dan informasi (Yampolskiy dkk., 2021). Kerahasiaan menekankan bahwa data hanya tersedia untuk individu yang berwenang. Integritas berkaitan dengan menjaga kebenaran dan keaslian data untuk mencegah perubahan ilegal, sedangkan ketersediaan menggarisbawahi perlunya data dan sistem untuk segera tersedia sesuai kebutuhan selama proses perawatan kesehatan.

Sejumlah studi global tentang keamanan data kesehatan menunjukkan bahwa transformasi digital layanan kesehatan memperkuat kebutuhan akan penetapan standar perlindungan data yang komprehensif dan terintegrasi untuk menjaga kerahasiaan informasi dan memastikan keberlanjutan layanan kesehatan (Mishra dkk., 2024). Lebih jauh lagi, beberapa studi telah menunjukkan bahwa keamanan Rekam Medis Elektronik (EMR) dipengaruhi tidak hanya oleh faktor teknologi tetapi juga oleh kebijakan organisasi, kualitas sumber daya manusia, dan kesiapan infrastruktur pendukung. Penelitian oleh Setyaningrum dan Ricky menunjukkan adanya konflik antara kemampuan teknologi dan kebijakan organisasi, dan tingkat kesadaran pengguna merupakan hambatan utama dalam implementasi keamanan data berbasis CIA Triad

pada sistem RME (Esti Setyaningrum & Verry Ricky, 2025). Selain itu, hasil literature review mengenai keamanan RME menegaskan perlunya pelaksanaan evaluasi sistem keamanan secara berkala sebagai langkah preventif untuk meminimalkan risiko kebocoran data maupun serangan siber di fasilitas pelayanan kesehatan (Febriyana & Ichwani, 2024). Temuan penelitian di RSUD Patut Patuh Patju Gerung Lombok Barat menunjukkan masih terdapat berbagai kendala dalam implementasi RME, antara lain terjadinya kesalahan sistem (system error), duplikasi data, kelengkapan diagnosis yang belum optimal, serta belum dilakukannya pembaruan terhadap standar prosedur operasional terkait keamanan data RME (Kesehatan et al., 2025). Sementara itu, penelitian mengenai keamanan infrastruktur RME di RSUD Kabupaten Kediri mengidentifikasi bahwa kesiapan jaringan dan mekanisme perlindungan sistem masih menjadi tantangan dalam penyelenggaraan rekam medis elektronik (Jayanto et al., 2025). Hasil penelitian di RSUD Welas Asih juga mengungkapkan bahwa ketidakstabilan jaringan internet merupakan permasalahan utama yang dihadapi, sehingga dilakukan peningkatan kapasitas server sebagai upaya perbaikan yang berkaitan dengan aspek availability dalam sistem RME (Dwi Setiyawan et al., 2025).

Hasil observasi pendahuluan yang dilakukan di Puskesmas Cempaka Putih Kota Banjarmasin menunjukkan adanya beberapa kondisi yang berpotensi memengaruhi tingkat keamanan data Rekam Medis Elektronik (RME), di antaranya praktik penggunaan akun secara bersama oleh beberapa poli, pengendalian terhadap akses pengguna yang belum berjalan secara optimal, keterbatasan prosedur penanganan saat Sistem sedang mengalami gangguan, dan jejak audit yang tidak memadai saat ini tidak tersedia pada sistem yang digunakan. Keadaan ini dapat memengaruhi kerahasiaan, integritas, dan ketersediaan data pasien dalam pelaksanaan pelayanan kesehatan sehari-hari. Penelitian ini dilakukan untuk mengevaluasi implementasi keamanan data dalam sistem Rekam Medis Elektronik sesuai dengan prinsip CIA di Puskesmas Cempaka Putih, Kota Banjarmasin.

METODE

Penelitian ini menggunakan metodologi deskriptif dengan pendekatan kualitatif untuk menganalisis atribut keamanan data sistem Rekam Medis Elektronik (EMR) di Puskesmas Cempaka Putih, Kota Banjarmasin. Metode kualitatif digunakan untuk memperoleh pengetahuan komprehensif tentang implementasi keamanan informasi yang berlandaskan prinsip Triad CIA yaitu kerahasiaan, integritas, dan ketersediaan. Penelitian ini dilakukan di Puskesmas Cempaka Putih, Kota Banjarmasin dari April hingga Juni 2026. Subjek penelitian terdiri dari individu yang bertanggung jawab atas pendaftaran dan rekam medis, petugas pendaftaran, dan praktisi kesehatan yang terlibat dalam penggunaan sistem tersebut. Subjek penelitian adalah sistem Rekam Medis Elektronik (EMR) yang digunakan dalam pemberian layanan kesehatan.

Tahap penelitian meliputi identifikasi masalah, tujuan penelitian, karakteristik informan, pengumpulan data, analisis data, hasil, dan diskusi. Gambar 1 mengilustrasikan urutan komprehensif dari tahap penelitian



Gambar 1. Alur Tahapan Penelitian

1. Identifikasi Masalah: Fase awal penelitian ini melibatkan pengenalan berbagai masalah yang terkait dengan penerapan keamanan data dalam sistem Rekam Medis Elektronik (EMR). Prosedur identifikasi melibatkan pengamatan awal dan penilaian kondisi saat ini untuk mengevaluasi implementasi keamanan data sesuai dengan prinsip Triad CIA.
2. Penetapan Tujuan Studi: Pada fase ini, tujuan studi ditetapkan, khususnya untuk meneliti pelaksanaan keamanan data terkait bidang Kerahasiaan, Integritas, dan Ketersediaan di Puskesmas Cempaka Putih di Kota Banjarmasin.
3. Identifikasi Karakteristik Informan: Informan penelitian diidentifikasi dengan metode sampel bertujuan, memilih individu yang secara langsung terlibat dalam pengelolaan dan pemanfaatan sistem.
4. Pengumpulan Data: Data penelitian diperoleh melalui pengamatan langsung terhadap sistem dan proses manajemen Rekam Medis Elektronik, wawancara komprehensif dengan informan terpilih, analisis kebijakan dan prosedur yang relevan, dan tinjauan literatur yang berkaitan dengan topik penelitian.
5. Hasil dan Diskusi: Bagian ini menekankan penyajian dan analisis temuan studi tentang penerapan keamanan data Rekam Medis Elektronik, khususnya membahas dimensi Kerahasiaan, Integritas, dan Ketersediaan. Data tersebut kemudian diperiksa dan dibandingkan dengan gagasan, standar, dan hasil studi sebelumnya untuk mendapatkan pemahaman yang lebih menyeluruh tentang subjek yang diteliti.
6. Kesimpulan : Menyimpulkan hasil temuan penelitian.

E-ISSN: 2865-6583
P-ISSN: 2868-6298
10.52643/marsi.v10i4.9111

HASIL DAN PEMBAHASAN

Penelitian ini dimulai dengan mengidentifikasi isu-isu untuk memberikan gambaran umum tentang status implementasi keamanan informasi yang ada dalam sistem Rekam Medis Elektronik (EMR) di Puskesmas Cempaka Putih, Kota Banjarmasin. Hasil penelitian menunjukkan bahwa pelaksanaan keamanan informasi di dalam sistem EMR masih menghadapi beberapa tantangan yang perlu dipertimbangkan. Salah satu pengamatan adalah penggunaan akun bersama oleh banyak petugas dan unit layanan. Kondisi tersebut terjadi karena akun yang tersedia digunakan secara bergantian untuk mempercepat proses pelayanan kepada pasien. Temuan berikutnya menunjukkan bahwa pengendalian terhadap hak akses pengguna belum sepenuhnya berjalan secara optimal. Konfigurasi hak akses dalam sistem masih belum selaras dengan tugas dan tanggung jawab setiap pengguna, sesuai dengan prinsip hak akses minimal (least privilege), yaitu pemberian hak akses sesuai kebutuhan pekerjaan. Kondisi tersebut berpotensi membuka peluang bagi pengguna untuk mengakses informasi yang tidak berkaitan dengan kewenangan maupun fungsi kerjanya.

Dengan demikian, hasil identifikasi masalah menunjukkan bahwa masih terdapat beberapa aspek keamanan informasi yang perlu dievaluasi lebih lanjut melalui analisis berdasarkan kerangka CIA Triad.

1. Karakterisik Informan

Penelitian ini melibatkan empat informan yang dipilih melalui pengambilan sampel bertujuan karena keahlian dan keterlibatan mereka dengan sistem Rekam Medis Elektronik (EMRS) di Puskesmas Cempaka Putih, Kota Banjarmasin. Informan dipilih berdasarkan tanggung jawab spesifik mereka dalam proses manajemen pencatatan, penginputan, serta pemanfaatan data rekam medis elektronik dalam pelayanan kesehatan sehari-hari.

Tabel 1. Karakteristik Informan Penelitian

Jabatan	**Pendidikan**	**Masa Kerja**
PJ Rekam Medis	D3 RMIK	5 tahun
Petugas Pendaftaran	SMA	11 tahun
Dokter	Profesi Kedokteran	7 tahun
Perawat	D3 Keperawatan	17 tahun

Sumber: Data Penelitian, 2026

Berdasarkan Tabel 1, partisipan penelitian terdiri dari empat orang dengan tanggung jawab berbeda dalam pemanfaatan Sistem Rekam Medis Elektronik (EMRS) di Puskesmas Cempaka Putih, Kota

Banjarmasin. Informan dipilih secara sengaja berdasarkan keterlibatan langsung mereka dalam administrasi dan penggunaan sistem EMR. Informan tersebut mencakup aspek manajemen rekam medis, personel administrasi, dan tenaga profesional kesehatan, termasuk dokter dan perawat. Latar belakang pendidikan dan masa kerja informan yang beragam menawarkan berbagai sudut pandang tentang implementasi keamanan data sesuai dengan prinsip Kerahasiaan, Integritas, dan Ketersediaan (CIA Triad). Pengalaman kerja informan, yang berkisar antara 5 hingga 17 tahun, dianggap memadai untuk memberikan wawasan komprehensif tentang metode manajemen keamanan data, pemanfaatan sistem, dan berbagai tantangan yang dihadapi dalam penerapan EMRS di dalam puskesmas.

Informan pertama merupakan Penanggung Jawab Pendaftaran dan Rekam Medis yang memiliki tugas dalam pengelolaan pelayanan pendaftaran, pengawasan pelaksanaan rekam medis, serta koordinasi penggunaan sistem RME. Informan ini dipilih karena memiliki pemahaman yang komprehensif mengenai kebijakan, pengelolaan hak akses pengguna, prosedur koreksi data, serta mekanisme keamanan informasi yang diterapkan pada sistem.

Informan kedua Petugas Pendaftaran yang berperan sebagai pengguna awal sistem dalam proses registrasi pasien dan pengelolaan data identitas. Keterlibatan informan ini memberikan informasi mengenai implementasi keamanan data pada tahap input data, penggunaan akun pengguna, serta penerapan pengendalian akses dalam operasional pelayanan.

Informan ketiga merupakan Dokter yang memanfaatkan sistem RME untuk melakukan pencatatan hasil pemeriksaan, penegakan diagnosis, serta dokumentasi tindakan medis. Informasi yang diberikan oleh informan ini penting untuk menggambarkan implementasi keamanan data dari perspektif tenaga medis sebagai pengguna utama data klinis pasien.

Informan keempat Perawat yang berperan dalam pendokumentasian pelayanan keperawatan serta pemanfaatan data pasien dalam proses pelayanan kesehatan. Partisipasi para informan ini sangat penting untuk mendapatkan pemahaman komprehensif tentang pemanfaatan sistem di tingkat layanan langsung dan untuk memahami masalah keamanan data yang berkaitan dengan aktivitas pencatatan dan akses informasi pasien.

Beragamnya latar belakang dan peran informan penelitian menghasilkan data yang lebih luas mengenai pelaksanaan pengamanan data dalam Sistem Rekam Medis Elektronik. Penelitian ini, berdasarkan wawasan dari pengelola rekam medis, tenaga administrasi, dan profesional kesehatan, secara efektif menjelaskan penerapan prinsip kerahasiaan, integritas, dan ketersediaan dalam pemberian layanan kesehatan di Puskesmas Cempaka Putih Kota Banjarmasin.

Pemeriksaan temuan penelitian dilakukan sehubungan dengan tiga elemen utama prinsip Triad CIA: kerahasiaan, integritas, dan ketersediaan. Temuan penelitian yang diperoleh dari observasi, wawancara

komprehensif, dan analisis dokumen mengenai penerapan sistem Rekam Medis Elektronik (EMR) di Puskesmas Cempaka Putih Kota Banjarmasin adalah sebagai berikut:

2. Pengumpulan Data

Pengumpulan data dilaksanakan secara bertahap di Puskesmas Cempaka Putih Kota Banjarmasin setelah peneliti memperoleh izin pelaksanaan penelitian dari instansi terkait. Proses pengumpulan data mengombinasikan teknik wawancara mendalam, observasi, dan telaah dokumen untuk memperoleh gambaran yang utuh mengenai penerapan keamanan data pada sistem Rekam Medis Elektronik (RME) berdasarkan aspek *Confidentiality*, *Integrity*, dan *Availability* (CIA Triad).

Data primer diperoleh melalui wawancara komprehensif dengan empat narasumber yang dipilih melalui pengambilan sampel bertujuan. Pemilihan informan didasarkan pada keterlibatan langsung mereka dalam penggunaan dan administrasi sistem EMR, sehingga memungkinkan mereka untuk memberikan informasi yang relevan dengan tujuan penelitian. Informan tersebut meliputi seorang manajer rekam medis, seorang petugas registrasi, seorang dokter, dan seorang perawat. Wawancara dilakukan secara langsung dengan menggunakan panduan wawancara semi-terstruktur yang disusun berdasarkan indikasi penelitian.

Selain wawancara, observasi dilakukan secara nonpartisipatif terhadap pelaksanaan penggunaan sistem RME dalam kegiatan pelayanan. Observasi difokuskan pada mekanisme autentikasi pengguna, pengelolaan hak akses, penggunaan akun oleh pengguna, pemanfaatan fitur keamanan sistem, serta praktik pengelolaan data yang berkaitan dengan kerahasiaan, keutuhan, dan ketersediaan informasi rekam medis elektronik. Seluruh hasil pengamatan dicatat secara sistematis menggunakan lembar observasi yang telah disusun sebelum penelitian dilaksanakan.

Data penelitian diperkaya dengan memeriksa dokumen-dokumen yang berkaitan dengan implementasi keamanan informasi di Puskesmas, termasuk prosedur operasi standar (SOP), kebijakan penggunaan sistem informasi, dan dokumen pendukung tambahan yang relevan dengan manajemen EMR. Temuan dari tinjauan dokumen berfungsi sebagai bukti penguat untuk memvalidasi informasi yang diperoleh dari wawancara dan observasi.

Metode pengumpulan data dilanjutkan secara terus-menerus hingga muncul pola yang konsisten dan tidak ditemukan informasi baru yang bermakna. Untuk memperkuat kredibilitas temuan penelitian, para peneliti menggunakan triangulasi teknis dengan membandingkan hasil dari wawancara, observasi, dan analisis dokumen, bersamaan dengan triangulasi sumber dengan membandingkan informasi yang diberikan oleh setiap informan berdasarkan peran dan tanggung jawab mereka dalam mengelola Rekam Medis Elektronik.

3. Analisis Data

Analisis data dilakukan secara bersamaan dengan pengumpulan data, memungkinkan pemeriksaan berkelanjutan terhadap materi yang dikumpulkan untuk memperoleh pemahaman menyeluruh tentang

fenomena yang diteliti. Studi ini menggunakan kerangka kerja analisis data interaktif yang dikembangkan oleh Miles, Huberman, dan Saldaña, yang mencakup kondensasi data, presentasi data, dan formulasi serta validasi kesimpulan.

Fase kondensasi data dimulai dengan pemeriksaan semua hasil wawancara, catatan observasi, dan dokumen yang dikumpulkan. Rekaman wawancara ditranskripsikan secara verbatim, kemudian dilakukan seleksi, kategorisasi, dan penyederhanaan. Data yang berkaitan dengan Kerahasiaan, Integritas, dan Ketersediaan dikategorikan sesuai dengan itu, sementara informasi yang tidak relevan dengan tujuan penelitian dihilangkan dari analisis.

Fase selanjutnya melibatkan presentasi data, menyusun hasil analisis ke dalam deskripsi naratif, matriks, dan tabel tema untuk secara sistematis memahami keterkaitan antar temuan. Penyajian data dilakukan berdasarkan masing-masing komponen CIA Triad untuk menggambarkan kondisi keamanan data Rekam Medis Elektronik, meliputi upaya menjaga kerahasiaan informasi, mekanisme pemeliharaan keutuhan data, serta ketersediaan data dalam mendukung pelayanan kesehatan.

Tahap terakhir berupa penarikan dan verifikasi kesimpulan dilakukan melalui proses penafsiran terhadap seluruh temuan penelitian dengan membandingkan hasil wawancara, observasi, dan telaah dokumen. Kesimpulan disusun setelah ditemukan pola, keterkaitan, dan konsistensi informasi antarsumber data. Proses verifikasi dilakukan secara berulang selama penelitian berlangsung untuk memastikan bahwa interpretasi yang dihasilkan sesuai dengan data empiris yang diperoleh di lapangan dan mampu menjawab tujuan penelitian mengenai implementasi keamanan Rekam Medis Elektronik berdasarkan aspek *Confidentiality*, *Integrity*, dan *Availability*.

4. Hasil dan Pembahasan

Hasil penelitian disajikan berdasarkan tiga aspek utama dalam kerangka *Confidentiality*, *Integrity*, dan *Availability* (CIA Triad). Penyajian temuan dilakukan melalui triangulasi data yang diperoleh dari wawancara mendalam, observasi, dan telaah dokumentasi. Setiap aspek dianalisis berdasarkan indikator penelitian untuk menggambarkan kondisi implementasi keamanan data Rekam Medis Elektronik (RME) di Puskesmas Cempaka Putih Kota Banjarmasin. Ringkasan temuan penelitian pada masing-masing aspek disajikan pada tabel berikut.

a. Aspek *Confidentiality* (Kerahasiaan)

Tabel 2. Temuan Penelitian Aspek *Confidentiality* (Kerahasiaan)

Indikator	Temuan Utama
Pengelolaan akun	Masih terdapat penggunaan akun bersama.

Hak akses	Hak akses telah disesuaikan dengan tugas pengguna.
Password	Sistem mewajibkan pergantian password setiap tiga bulan.
Auto logout	Belum tersedia fitur *auto logout*.
Kebijakan keamanan	Sosialisasi keamanan informasi belum dilakukan secara berkala

Confidentiality merupakan prinsip yang bertujuan untuk melindungi informasi agar tidak dapat diakses maupun diungkapkan kepada pihak atau sistem yang tidak memiliki kewenangan (Wahyu Wijaya Widiyanto, 2025). Hasil penelitian menunjukkan bahwa upaya menjaga kerahasiaan data telah diterapkan melalui mekanisme penggunaan username dan password pada sistem Rekam Medis Elektronik. Meskipun demikian, penerapan akun pengguna belum sepenuhnya dilakukan secara individual karena sebagian akun masih digunakan berdasarkan poli pelayanan. Salah satu informan menyampaikan bahwa "username dibuat perpoli, ada juga dibuat perorangan". Temuan tersebut mengindikasikan bahwa mekanisme autentikasi yang diterapkan belum sepenuhnya memenuhi prinsip *confidentiality* dalam keamanan informasi. Sejalan dengan hal tersebut, penelitian yang dilakukan oleh Diva Rizky *et al.* menjelaskan bahwa penggunaan username dan password secara bersama-sama dapat menimbulkan risiko yang signifikan karena menyulitkan proses audit dalam mengidentifikasi pihak yang bertanggung jawab apabila terjadi kesalahan pada input data (Rizky Amanda Tiorentap, 2020).

Penggunaan akun secara bersama-sama oleh beberapa petugas masih ditemukan pada sejumlah unit pelayanan. Berdasarkan keterangan informan, "akun dibuatkan per poli". Praktik tersebut berpotensi menimbulkan permasalahan dalam proses identifikasi pengguna apabila terjadi perubahan data ataupun penyalahgunaan akses terhadap informasi yang tersimpan dalam sistem. Selain itu, hasil observasi memperlihatkan bahwa masih terdapat password yang ditempel pada beberapa area kerja, sehingga dapat meningkatkan kemungkinan terjadinya akses tanpa otorisasi terhadap data pasien.

Di sisi lain, sistem telah menerapkan kebijakan perubahan password secara berkala setiap tiga bulan melalui mekanisme otomatis yang tersedia pada aplikasi ePuskesmas. Salah satu informan menyampaikan bahwa "3 bulan sekali sistem rekam medis elektronik otomatis mewajibkan penggantian password". Temuan tersebut menunjukkan adanya upaya untuk memperkuat keamanan akses pengguna dalam sistem. Hasil ini sejalan dengan penelitian Suhariyono *et al*. yang menyatakan bahwa pergantian password setiap tiga bulan dilakukan sebagai langkah untuk menjaga keamanan data pada aplikasi (Suhariyono et al., 2025).

Namun demikian, fitur *log out* otomatis masih belum tersedia pada sistem Rekam Medis Elektronik di Puskesmas Cempaka Putih. Keberadaan fitur tersebut memiliki peran penting dalam mencegah akses oleh pihak yang tidak memiliki kepentingan terhadap data yang tersimpan dalam sistem (Suhariyono et al., 2025). Penelitian yang dilakukan oleh Tiorentap et al. (2020) juga menegaskan bahwa penerapan *log out* otomatis merupakan salah satu mekanisme yang dapat memperkuat aspek *confidentiality* dalam keamanan informasi (Rizky Amanda Tiorentap, 2020).

Penerapan pembatasan hak akses pada sistem telah disesuaikan dengan tugas dan kewenangan masing-masing tenaga kesehatan. Akses diberikan kepada petugas yang terlibat secara langsung dalam proses pelayanan, seperti dokter, perawat, serta tenaga kesehatan lainnya. Meskipun demikian, berdasarkan hasil wawancara diketahui bahwa masih terdapat beberapa pengaturan hak akses yang perlu disempurnakan. Salah satu kondisi yang ditemukan adalah akun dokter yang masih memiliki kemampuan untuk melakukan pendaftaran pasien secara langsung, sehingga menunjukkan perlunya penyesuaian hak akses agar lebih sesuai dengan fungsi dan tanggung jawab pengguna.

Upaya perlindungan terhadap kerahasiaan data pasien yang diterapkan saat ini masih tergolong sederhana dan belum didukung oleh regulasi yang kuat maupun kegiatan sosialisasi khusus terkait keamanan data. Padahal, sosialisasi dan edukasi merupakan langkah yang penting dalam meningkatkan perlindungan data serta mengurangi potensi terjadinya pelanggaran keamanan informasi (Destri Maya Rani et al., 2024).

b. Aspek *Integrity* (Integritas)

Tabel 3. Temuan Penelitian Aspek *Integrity* (Keutuhan Data)

Indikator	Temuan Utama
Perubahan data	Terdapat SOP tentang perubahan data dilakukan 2 x 24 jam.
Audit Trail	Terdapat fitur audit trail namun belum mencatat semua aktivitas perubahan.
Keakuratan data	Koreksi data hanya dapat dilakukan oleh petugas yang memiliki kewenangan tertentu.

Integrity atau integritas data merupakan prinsip yang menekankan pemeliharaan konsistensi, ketepatan, dan keandalan data selama seluruh siklus hidupnya. Data harus terlindungi dari perubahan yang tidak sah maupun modifikasi yang tidak dapat terdeteksi. Dalam konteks pelayanan kesehatan, aspek integritas memiliki peranan yang sangat penting karena perubahan data tanpa kewenangan, seperti informasi dosis obat, riwayat alergi, maupun diagnosis pasien, dapat menimbulkan konsekuensi yang serius. Untuk menjaga integritas data, sistem umumnya menerapkan berbagai mekanisme pengamanan,

antara lain checksums, tanda tangan digital *(digital signatures*), serta audit trail yang berfungsi mencatat setiap perubahan data, pihak yang melakukan perubahan, dan waktu terjadinya perubahan tersebut (Yoder, 2025).

Hasil penelitian menunjukkan bahwa Puskesmas Cempaka Putih telah menerapkan prosedur perbaikan data sesuai dengan Prosedur Operasi Standar (SOP) internal. Koreksi data hanya diperbolehkan dalam jangka waktu 48 jam melalui mekanisme penundaan dan memerlukan persetujuan dari petugas rekam medis yang berwenang. Temuan ini sesuai dengan penelitian yang dilakukan oleh Suhariyono dkk. (2025), yang menunjukkan bahwa penghapusan data hanya diperbolehkan oleh kepala rekam medis, yang bertindak sebagai administrator sistem [20]. Batas waktu modifikasi data 2 x 24 jam sesuai dengan Peraturan Menteri Kesehatan No. 24 Tahun 2022 tentang Rekam Medis, yang mewajibkan perubahan data harus dilakukan dalam waktu 2 x 24 jam setelah entri awal ke dalam sistem (Peraturan Menteri Kesehatan No. 24 Tahun 2022 tentang Rekam Medis, n.d.-b).

Selain itu, temuan penelitian menunjukkan bahwa fitur jejak audit dalam sistem Rekam Medis Elektronik (EMR) di Puskesmas Cempaka Putih tidak beroperasi pada tingkat yang dapat diterima. Sistem tersebut hanya menyajikan informasi mengenai nama pengguna terbaru yang melakukan modifikasi data, tanpa memberikan catatan aktivitas pengguna yang komprehensif dan detail. Kesimpulan ini diperkuat oleh data wawancara, yang menunjukkan bahwa “hanya sebatas tercatat terakhir diubah oleh username petugas”, serta hasil observasi yang menunjukkan bahwa sistem belum dapat menyajikan riwayat perubahan data *(history log*) secara menyeluruh. Kondisi ini menunjukkan bahwa implementasi audit trail masih terbatas pada identifikasi pengguna terakhir yang melakukan perubahan dan belum mampu mendukung proses penelusuran aktivitas pengguna secara rinci dalam pengelolaan data rekam medis.

Secara teoritis, audit trail merupakan salah satu komponen yang memiliki peran penting dalam keamanan sistem informasi kesehatan karena berfungsi mendokumentasikan seluruh aktivitas pengguna secara kronologis. Informasi yang dicatat meliputi waktu akses, jenis aktivitas yang dilakukan, data yang mengalami perubahan, serta identitas pengguna yang melakukan tindakan tersebut. Keberadaan pencatatan tersebut diperlukan untuk menjamin akuntabilitas, transparansi, dan integritas data dalam sistem Rekam Medis Elektronik. Penelitian yang dipublikasikan oleh *Journal of the American Medical Informatics Association* (JAMIA) menjelaskan bahwa audit log pada sistem Rekam Medis Elektronik seharusnya mampu merekam seluruh aktivitas pengguna secara berurutan (*time-sequenced record*), sehingga dapat dimanfaatkan untuk menelusuri perubahan data sekaligus mengevaluasi penggunaan sistem secara menyeluruh (Kannampallil & Adler-Milstein, 2023).

Hasil penelitian ini menunjukkan kesesuaian dengan temuan pada penelitian *Analisis Penerapan Audit Trail pada Rekam Medis Elektronik di Rumah Sakit X Jawa Tengah*, yang mengungkapkan bahwa fitur audit trail belum mampu mendokumentasikan perubahan data secara terperinci, terutama pada perubahan kode diagnosis dan tindakan medis. Keterbatasan tersebut mengakibatkan proses penelusuran riwayat perubahan data menjadi kurang optimal serta berpotensi mengurangi tingkat akuntabilitas sistem. Penelitian tersebut juga menegaskan bahwa audit trail yang efektif harus dapat menyajikan riwayat perubahan data secara kronologis sehingga seluruh aktivitas pengguna yang terjadi dalam sistem dapat ditelusuri secara jelas dan terdokumentasi dengan baik (Dewi & Ricky, 2025).

c. Aspek *Availability* (Ketersediaan)

Tabel 3. Temuan Penelitian Aspek *Availability* (Ketersediaan Data)

Indikator	Temuan Utama
Ketersediaan sistem	Sistem memiliki tingkat ketersediaan yang cukup baik, tetapi stabilitas jaringan masih menjadi faktor yang memengaruhi kelancaran pelayanan.
Backup data	Informan menjelaskan bahwa pencadangan data dilakukan secara berkala oleh pengelola sistem.
Pemulihan layanan	Mekanisme penanganan gangguan telah tersedia sehingga mendukung keberlangsungan pelayanan, meskipun waktu pemulihan masih dipengaruhi oleh jenis gangguan yang terjadi.
Sumber listrik cadangan	Terdapat genset sebagai alternatif cadangan jika terjadi pemadaman listrik

Availability atau ketersediaan merupakan prinsip yang memastikan bahwa informasi dan sistem dapat diakses serta digunakan secara tepat waktu oleh pengguna yang memiliki kewenangan (Wahyu Wijaya Widiyanto, 2025). Hasil penelitian menunjukkan bahwa sistem Rekam Medis Elektronik (RME) di Puskesmas Cempaka Putih Kota Banjarmasin pada umumnya telah mendukung pelaksanaan pelayanan kesehatan sehari-hari. Melalui sistem tersebut, prose pencatatan dan pengelolaan data pasien dapat dilakukan secara elektronik sehingga berkontribusi terhadap peningkatan efektivitas pelayanan kesehatan

(*Global Strategy on Digital Health 2020-2025*, 2021). Meskipun demikian, berdasarkan hasil wawancara, diketahui bahwa ketika terjadi gangguan sistem atau *downtime*, akses terhadap RME menjadi tidak tersedia sehingga aktivitas pelayanan yang bergantung pada sistem tersebut mengalami kendala dan harus dialihkan menggunakan prosedur alternatif. Temuan ini menunjukkan bahwa aspek ketersediaan (*availability*) masih sangat bergantung pada keandalan aplikasi serta infrastruktur teknologi informasi yang mendukung operasional sistem.

Dalam kerangka CIA Triad, aspek *availability* menekankan pentingnya memastikan bahwa informasi dan sistem selalu berada dalam kondisi tersedia serta dapat diakses oleh pengguna yang berwenang ketika diperlukan untuk mendukung keberlangsungan aktivitas organisasi (Whitman & Mattord, 2018). Penelitian Larsen et al. menunjukkan bahwa terjadinya *downtime* pada sistem Rekam Medis Elektronik dapat memberikan dampak yang signifikan terhadap operasional pelayanan kesehatan, antara lain keterlambatan proses pelayanan, meningkatnya beban kerja petugas, terganggunya komunikasi antarunit, serta munculnya potensi risiko terhadap keselamatan pasien. Penelitian tersebut juga menegaskan bahwa fasilitas pelayanan kesehatan perlu memiliki perencanaan kontinjensi yang lebih komprehensif, terutama yang berkaitan dengan mekanisme komunikasi, pengelolaan sumber daya, pelatihan petugas, serta prosedur penanganan *downtime*, guna memastikan pelayanan kesehatan tetap berlangsung secara aman dan efektif (Larsen et al., 2019).

Berdasarkan hasil penelitian, ketersediaan jaringan internet di Puskesmas Cempaka Putih dapat dikategorikan cukup memadai karena didukung oleh dua jaringan Wi-Fi yang berasal dari sumber berbeda dan berfungsi sebagai koneksi utama serta koneksi cadangan. Penerapan lebih dari satu layanan internet menunjukkan adanya mekanisme *redundancy* yang dirancang untuk meningkatkan keandalan sistem sekaligus meminimalkan risiko terganggunya layanan apabila salah satu jaringan mengalami gangguan (NIST TEAM, 2024). National Institute of Standards and Technology (NIST) menyebutkan bahwa penerapan redundansi pada infrastruktur teknologi informasi merupakan salah satu strategi penting untuk menjaga ketersediaan layanan serta mengurangi dampak yang ditimbulkan oleh kegagalan pada satu komponen sistem (*single point of failure*) (Swanson et al., 2010). Selain itu, hasil penelitian juga menunjukkan bahwa puskesmas telah menyediakan genset sebagai sumber daya listrik cadangan untuk mengantisipasi terjadinya pemadaman listrik. Ketersediaan sumber listrik alternatif tersebut menjadi bagian dari strategi mitigasi risiko yang berperan penting dalam menjaga keberlangsungan operasional sistem informasi kesehatan. Dengan adanya jaringan internet cadangan dan genset, dapat diketahui bahwa organisasi telah memiliki dukungan infrastruktur yang cukup baik dalam menunjang aspek *availability* pada sistem Rekam Medis Elektronik (*Global Strategy on Digital Health 2020-2025*, 2021).

Selain faktor infrastruktur, hasil penelitian juga memperlihatkan bahwa puskesmas telah menerapkan mekanisme penanganan gangguan sistem melalui koordinasi dengan vendor aplikasi apabila terjadi kendala teknis. Berdasarkan keterangan informan, ketika proses perbaikan sistem membutuhkan waktu yang cukup lama, pelayanan kesehatan tetap dilaksanakan secara manual agar proses pelayanan kepada pasien tidak mengalami penghentian. Praktik tersebut sejalan dengan rekomendasi World Health Organization (WHO) yang menekankan pentingnya penerapan prosedur alternatif (*contingency procedures*) untuk memastikan keberlangsungan pelayanan kesehatan selama terjadi gangguan pada teknologi informasi yang digunakan (*Global Strategy on Digital Health 2020-2025*, 2021).

Temuan penting yang diperoleh dalam penelitian ini menunjukkan bahwa Puskesmas Cempaka Putih belum memiliki Standar Operasional Prosedur (SOP) khusus yang mengatur penanganan *downtime* pada sistem Rekam Medis Elektronik. Berdasarkan hasil wawancara, informan menyatakan bahwa hingga penelitian ini dilaksanakan belum tersedia prosedur tertulis yang dapat dijadikan pedoman resmi ketika sistem mengalami gangguan. Kondisi tersebut mengindikasikan masih adanya kelemahan dalam tata kelola keamanan informasi, terutama yang berkaitan dengan kesiapan teknologi informasi dan keberlangsungan layanan. Dalam ISO/IEC 27001:2022, *ICT readiness for business continuity* ditetapkan sebagai salah satu kontrol penting yang mengharuskan organisasi untuk merencanakan, menerapkan, memelihara, serta menguji kesiapan teknologi informasi guna mendukung kontinuitas proses bisnis pada saat terjadi gangguan sistem (Vakhula et al., 2024). Sejalan dengan hal tersebut, Vakhula et al. menjelaskan bahwa pembaruan ISO/IEC 27001:2022 semakin menekankan pentingnya kesiapan teknologi informasi sebagai faktor pendukung keberlangsungan operasional organisasi (Vakhula et al., 2024).

Keberadaan SOP *downtime* menjadi elemen penting yang berfungsi sebagai pedoman bagi petugas dalam melaksanakan pencatatan manual, mengelola data selama sistem mengalami gangguan, menjalankan proses pemulihan layanan, serta melakukan sinkronisasi data setelah sistem kembali beroperasi secara normal [28]. Larsen et al. menyatakan bahwa fasilitas pelayanan kesehatan perlu memiliki prosedur *downtime* yang terdokumentasi dengan jelas, disertai pelatihan rutin bagi petugas dan mekanisme komunikasi yang terstruktur, sehingga kesinambungan pelayanan tetap dapat dipertahankan ketika sistem elektronik tidak dapat digunakan (Larsen et al., 2019).

Secara umum, hasil penelitian menunjukkan bahwa aspek *availability* pada sistem Rekam Medis Elektronik di Puskesmas Cempaka Putih telah didukung oleh keberadaan jaringan internet cadangan, sumber listrik alternatif, serta mekanisme koordinasi dengan vendor aplikasi dalam menangani gangguan sistem. Namun demikian, belum tersedianya SOP khusus yang mengatur penanganan *downtime* mengindikasikan bahwa kesiapan organisasi dalam menghadapi gangguan sistem masih memerlukan penguatan. Penyusunan dan penerapan SOP *downtime* yang komprehensif diharapkan dapat meningkatkan

kontinuitas pelayanan kesehatan, memperjelas pembagian peran dan tanggung jawab petugas selama terjadi gangguan sistem, serta mendukung implementasi prinsip *availability* dalam pengelolaan Rekam Medis Elektronik secara lebih optimal (*Global Strategy on Digital Health 2020-2025*, 2021).

KESIMPULAN

Hasil penelitian menunjukkan bahwa penerapan keamanan data pada sistem Rekam Medis Elektronik (RME) di Puskesmas Cempaka Putih Kota Banjarmasin telah mencakup tiga elemen utama dalam prinsip CIA Triad, yaitu *confidentiality*, *integrity*, dan *availability*. Meskipun demikian, implementasi ketiga aspek tersebut masih memerlukan berbagai penyempurnaan. Pada aspek *confidentiality*, sistem telah menerapkan mekanisme autentikasi melalui penggunaan *username* dan *password* serta pengaturan hak akses sesuai dengan tugas dan kewenangan pengguna. Namun, masih ditemukan praktik penggunaan akun secara bersama pada beberapa unit pelayanan, belum tersedianya fitur *log out* otomatis, serta belum adanya kebijakan dan kegiatan sosialisasi keamanan data yang tersusun secara sistematis. Kondisi tersebut berpotensi meningkatkan risiko terjadinya akses yang tidak sah terhadap data pasien.

Pada aspek *integrity*, sistem telah menerapkan mekanisme koreksi data yang mengacu pada prosedur operasional yang berlaku serta pembatasan waktu dalam melakukan perubahan data. Akan tetapi, fitur *audit trail* yang tersedia masih memiliki keterbatasan karena hanya mampu menampilkan identitas pengguna terakhir yang melakukan perubahan tanpa menyediakan riwayat aktivitas secara lengkap dan kronologis. Selain itu, pengaturan hak akses pengguna masih memerlukan penyesuaian agar lebih selaras dengan prinsip pemberian akses berdasarkan peran dan kebutuhan kerja. Temuan tersebut menunjukkan bahwa penguatan mekanisme akuntabilitas serta kemampuan pelacakan aktivitas pengguna masih diperlukan untuk menjaga integritas data pada sistem Rekam Medis Elektronik.

Pada aspek *availability*, sistem telah didukung oleh infrastruktur yang relatif memadai, antara lain berupa jaringan internet cadangan, sumber listrik alternatif, dan mekanisme koordinasi dengan vendor aplikasi dalam penanganan gangguan sistem. Namun demikian, belum tersedianya Standar Operasional Prosedur (SOP) khusus mengenai penanganan *downtime* menunjukkan bahwa kesiapan organisasi dalam menjaga kontinuitas layanan masih perlu ditingkatkan. Kondisi tersebut berpotensi memengaruhi keberlangsungan pelayanan kesehatan apabila terjadi gangguan sistem dalam jangka waktu tertentu.

Secara teoretis, hasil penelitian ini memperkuat pandangan bahwa keberhasilan penerapan keamanan data pada Rekam Medis Elektronik (RME) tidak semata-mata bergantung pada ketersediaan teknologi dan fitur keamanan yang digunakan, tetapi juga dipengaruhi oleh tata kelola organisasi, kebijakan keamanan informasi yang diterapkan, serta perilaku dan kesadaran pengguna dalam menjaga keamanan data. Dari perspektif praktis, penelitian ini memberikan gambaran mengenai kondisi aktual implementasi keamanan data RME pada fasilitas pelayanan kesehatan tingkat pertama yang dapat dimanfaatkan sebagai

bahan evaluasi dalam upaya peningkatan dan penyempurnaan sistem. Sementara itu, dari aspek kebijakan, temuan penelitian menegaskan pentingnya penguatan standar keamanan informasi, optimalisasi pengendalian hak akses pengguna, pengembangan audit trail yang lebih komprehensif, serta peningkatan kesiapan kontinuitas layanan sebagai upaya mendukung penyelenggaraan Rekam Medis Elektronik yang aman, andal, dan berkelanjutan.

DAFTAR PUSTAKA

[1]. Anggraeni, A., Ginting, J. G. A., & Ikhwan, S. (2022). Implementation of intrusion prevention system (IPS) to analysis triad cia on network security attacks on web server. *JURNAL INFOTEL*, *14*(4), 277–286. https://doi.org/10.20895/infotel.v14i4.813

[2]. Cholik, C. A. (2021). *Perkembangan Teknologi Informasi Komunikasi / ICT Dalam Berbagai Bidang* (Vol. 2, Number 2).

[3]. Destri Maya Rani, Bajeng Nurul Widyaningrum, & Lutfiyah Rizqulloh. (2024). Edukasi Mengenai Aspek Keamanan Informasi Data Pasien Pada Penerapan RME di RSI Sultan Agung. *Jurnal Pengabdian Kepada Masyarakat*, *1*(http://www.jurnal.faperta-unras.ac.id/index.php/pakdemas/issue/view/76), 115–120.

[4]. Dewi, N., & Ricky, A. V. (2025). Analisis Penerapan Audit Trail pada Rekam Medis Elektronik di Rumah Sakit X Jawa Tengah. *Jurnal Ners*, *9*, 4228–4236. http://journal.universitaspahlawan.ac.id/index.php/ners

[5]. Dwi Setiyawan, Y., Kesehatan, F., & TEDC Bandung, P. (2025). Tinjauan Keamanan Informasi Pasien Melalui Pemeliharaan Rekam Medis Elektronik Dalam Penyimpanan Digital di RSUD Welas Asih. *Jurnal Kesehatan Tambusai*, *6*(3), 10801–10805.

[6]. Esti Setyaningrum, A., & Verry Ricky, A. (2025). Analisis Keamanan Data Pasien Dalam Rekam Medis Elektronik Berdasarkan CIA Triad di RSUD X Jawa Tengah. *Jurnal Ners Universitas Pahlawan*. http://journal.universitaspahlawan.ac.id/index.php/ners

[7]. Gede, I., Agung, E., & Punia, A. (2024). *Aspek Hukum dan Pertanggungjawaban Keamanan Data Rekam Medis Elektronik di Indonesia*.

[8]. Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., & Jain, R. (2021). Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security. *IEEE Internet of Things Journal*, *8*(11), 8707–8718. https://doi.org/10.1109/JIOT.2020.3045653

[9]. *Global Strategy on Digital Health 2020-2025*. (2021). World Health Organization.

[10]. Herrera Montano, I., Góngora Alonso, S., Sañudo García, S., García Aranda, J. J., Rodrígues, J. J. P. C., & de la Torre Díez, I. (2026). Security practices and insider threats in Spanish

healthcare centers: a survey-based risk assessment. *International Journal of Medical Informatics*, *205*. https://doi.org/10.1016/j.ijmedinf.2025.106107

[11]. Jayanto, D. L., Herfin, M., Akbar, M., Saputra, S., Djusmin, V. Bin, Zuliana, N., Ardila, N. M. I., Poonwong, P., & Bawias, J. S. C. (2025). Kesiapan dan Keamanan Infrastruktur Penyelenggaraan Rekam Medis Elektronik di RSUD Kabupaten Kediri. *Jurnal Sains, Nalar, Dan Aplikasi Teknologi Informasi*, *4*(2), 157–164. https://doi.org/10.20885/snati.v4.i2.40288

[12]. Kagita, M. K., Thilakarathne, N., Gadekallu, T. R., & Maddikunta, P. K. R. (2022). *A Review on Security and Privacy of Internet of Medical Things* (pp. 171–187). https://doi.org/10.1007/978-3-030-81473-1_8

[13]. Kannampallil, T., & Adler-Milstein, J. (2023). Using electronic health record audit log data for research: Insights from early efforts. In *Journal of the American Medical Informatics Association* (Vol. 30, Number 1, pp. 167–171). Oxford University Press. https://doi.org/10.1093/jamia/ocac173

[14]. Febriyana, & Ichwani. (2024). *Keamanan Data Rekam Medis Elektronik Menggunakan Teknik Kriptografi : Literature Review*.

[15]. Kesehatan, J., Huda, Q., Septiana, A. P., Fatuhu, S., Komang, N., Yanti, W., & Khairan, F. (2025). *Tinjauan Keamanan Data Rekam Medis Elektronik Pasien di RSUD Patut Patuh Patju Gerung Lombok Barat*. *13*(2), 179–185. https://doi.org/10.37824/jkqh.v13i1.2025

[16]. Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security Techniques for the Electronic Health Records. *Journal of Medical Systems*, *41*(8). https://doi.org/10.1007/s10916-017-0778-4

[17]. Larsen, E., Hoffman, D., Rivera, C., Kleiner, B. M., Wernz, C., & Ratwani, R. M. (2019). Continuing Patient Care during Electronic Health Record Downtime. *Applied Clinical Informatics*, *10*(3), 495–504. https://doi.org/10.1055/s-0039-1692678

[18]. Mishra, V., Gupta, K., Saxena, D., & Singh, A. K. (2024). A Global Medical Data Security and Privacy Preserving Standards Identification Framework for Electronic Healthcare Consumers. *IEEE Transactions on Consumer Electronics*, *70*(1), 4379–4387. https://doi.org/10.1109/TCE.2024.3373912

[19]. NIST TEAM. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29

[20]. *Permenkes No 24 Tahun 2022 Tentang Rekam Medis*. (n.d.-a).

[21]. *Permenkes No 24 Tahun 2022 Tentang Rekam Medis*. (n.d.-b). Retrieved www.peraturan.go.id

[22]. Rizky Amanda Tiorentap, D. (2020). *Aspek Keamanan Informasi dalam Penerapan Rekam Medis Elektronik di Klinik Medical Check-Up MP*. SENWODIPA.

[23]. 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. https://doi.org/10.33560/jmiki.v13i1.812

[24]. Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). *Contingency planning guide for federal information systems*. https://doi.org/10.6028/NIST.SP.800-34r1

[25]. Tedjasukmana, D., & Riswadi, R. (2021). Legal Aspects of Medical Records and Data Security for Patients in Hospitals. *Proceedings of the 1st International Conference on Law, Social Science, Economics, and Education, ICLSSEE 2021, March 6th 2021, Jakarta, Indonesia*. https://doi.org/10.4108/eai.6-3-2021.2306400

[26]. Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in Biology and Medicine*, *129*, 104130. https://doi.org/10.1016/j.compbiomed.2020.104130

[27]. Vakhula, O., Kurii, Y., Opirskyy, I., & Susukailo, V. (2024). *Security-as-Code Concept for Fulfilling ISO/IEC 27001:2022 Requirements*.

[28]. Wahyu Wijaya Widiyanto. (2025). *Pertukaran Informasi Kesehatan* (Widiyanto, Ed.). Politeknik Indonusa Surakarta.

[29]. Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security Sixth Edition*. www.cengage.com.

[30]. Yampolskiy, M., Gatlin, J., & Yung, M. (2021). Myths and Misconceptions in Additive Manufacturing Security: Deficiencies of the CIA Triad. *AMSec 2021 - Proceedings of the 2021 Workshop on Additive Manufacturing (3D Printing) Security, Co-Located with CCS 2021*, 3–9. https://doi.org/10.1145/3462223.3485618

[31]. Yoder, D. (2025). Health information exchange. In Widiyanto (Ed.), *Information and Communication Technologies in Healthcare* (pp. 25–38). Politeknik Indonusa Surakarta. https://doi.org/10.1201/b11696-3