Journal of Health Information Management and Medical Record
Vol.2, No.1 (Juni) 2026, 23-29
E-ISSN: xxxx-xxxx
DOI: xx.xxxxx/xxxxx.xxxx.xxx
Journal homepage: https://e-journal.poltekkesjogja.ac.id/index.php/rmik/

Tinjauan keamanan data Rekam Medis Elektronik pada Aplikasi SIMRS berdasarkan aspek CIA Triad di RS Bhayangkara Polda DIY

Melvaya Shifa Roswidia[1], Abdul Hadi Kadarusno[2], Anton Kristijono[3]

[1]Rekam Medis dan Informasi Kesehatan Poltekkes Kemenkes Yogyakarta, Daerah Istimewa Yogyakarta 55143, melvaya12@gmail.com

[2]Rekam Medis dan Informasi Kesehatan Poltekkes Kemenkes Yogyakarta, Daerah Istimewa Yogyakarta 55143, abdul.hadik@poltekkesjogja.ac.id,

[3]Rekam Medis dan Informasi Kesehatan Poltekkes Kemenkes Yogyakarta, Daerah Istimewa Yogyakarta 55143, kristijonoanton@gmail.com

Kata Kunci

Keamanan Data
Rekam Medis Elektronik
SIMRS
CIA Triad

ABSTRAK

Latar Belakang: Rekam Medis Elektronik (RME) merupakan bagian dari digitalisasi pelayanan kesehatan yang memerlukan keamanan informasi untuk melindungi data pasien. Keamanan informasi didasarkan pada prinsip CIA Triad yang terdiri dari *confidentiality*, *integrity*, dan *availability*. RS Bhayangkara Polda DIY telah menerapkan Sistem Informasi Manajemen Rumah Sakit (SIMRS) sehingga diperlukan analisis keamanan data RME berdasarkan prinsip CIA Triad. **Tujuan:** Penelitian ini bertujuan untuk menganalisis keamanan data rekam medis elektronik pada aplikasi SIMRS berdasarkan aspek CIA Triad di RS Bhayangkara Polda DIY. **Metode:** Penelitian ini menggunakan metode deskriptif kualitatif. Pengumpulan data dilakukan melalui wawancara mendalam, observasi, dan studi dokumentasi. Informan berjumlah 10 orang, terdiri dari Kepala SIM dan RM, petugas administrasi/kasir, tenaga kesehatan dari beberapa unit pelayanan, serta satu informan triangulasi dari unit teknologi informasi. Analisis data dilakukan melalui kondensasi data, penyajian data, dan penarikan kesimpulan. **Hasil:** Pada aspek *confidentiality* telah diterapkan pengaturan hak akses melalui *username* dan *password* sesuai peran pengguna, namun masih ditemukan penggunaan akun secara bersama. Pada aspek *integrity* telah diterapkan pembatasan pengubahan data, validasi pengisian data, serta pembatasan waktu perubahan data. Pada aspek *availability* SIMRS telah terintegrasi antar unit pelayanan dan didukung *backup* data secara berkala, namun masih ditemukan kendala seperti gangguan sistem dan belum tersedianya UPS di beberapa unit. **Kesimpulan:** Penerapan keamanan data rekam medis elektronik pada aplikasi SIMRS berdasarkan aspek CIA Triad di RS Bhayangkara Polda DIY secara umum telah berjalan, namun belum sepenuhnya optimal. Diperlukan penguatan kebijakan keamanan data, penyusunan SOP khusus, peningkatan kesadaran pengguna, serta pengembangan infrastruktur teknologi.

Keyword:

ABSTRACT

Data Security
Electronic Medical Record
SIMRS
CIA Triad

Background: *Analysis of electronic medical record data security in the SIMRS application based on the CIA Triad aspects at Bhayangkara Hospital of Yogyakarta Regional Police. Background: Electronic Medical Records (EMR) are part of the digitalization of healthcare services and require information security to protect patient data. Information security is based on the CIA Triad principles, consisting of confidentiality, integrity, and availability. RS Bhayangkara Polda DIY has implemented a Hospital Management Information System (SIMRS); therefore, an analysis of EMR data security based on the CIA Triad principles is necessary.*

Objective: *This study aimed to analyze the security of electronic medical record data in the SIMRS application based on the CIA Triad aspects at Bhayangkara Hospital of Yogyakarta Regional Police.* ***Methods:*** *This study used a descriptive qualitative method. Data were collected through in-depth interviews, observations, and documentation. The informants consisted of 10 people, including the head of SIM and medical records, administration staff, health workers from several service units, and one triangulation informant from the information technology unit. Data were analyzed through data condensation, data presentation, and conclusion drawing.* ***Results:*** *The confidentiality aspect has been implemented through access control using usernames and passwords based on user roles, although account sharing among staff still occurs. The integrity aspect has been supported by restrictions on data editing, mandatory field validation, and time limitations for data changes. The availability aspect has been implemented through system integration between service units and periodic data backup, although system disruptions and the absence of UPS in some units were still found.* ***Conclusion:*** *The implementation of electronic medical record data security in the SIMRS application based on the CIA Triad aspects has generally been carried out but has not yet been fully optimal. Improvements are needed in the form of strengthening security policies, developing specific SOPs, increasing user awareness, and improving technological infrastructure.*

1. Pendahuluan

Di era globalisasi saat ini, kemajuan teknologi informasi (TI) berkembang pesat dan telah diterapkan di berbagai bidang, termasuk bidang kesehatan. Salah satu penerapan teknologi tersebut adalah Rekam Medis Elektronik (RME) pada Sistem Informasi Manajemen Rumah Sakit (SIMRS), yaitu solusi TI untuk mengumpulkan, menyimpan, memproses, dan mengakses data dalam sistem manajemen basis data [1]. Penggunaan sistem informasi dalam layanan kesehatan dapat meningkatkan mutu pelayanan, mengurangi kesalahan medis, dan meningkatkan kualitas pengambilan keputusan berbasis data [2]. Penyelenggaraan RME berdasarkan Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 mewajibkan fasilitas pelayanan kesehatan, termasuk rumah sakit, untuk menerapkan RME paling lambat 31 Desember 2023 [5]. Dalam pengelolaannya, prinsip keamanan data dan informasi meliputi kerahasiaan, integritas, dan ketersediaan harus diperhatikan untuk melindungi RME dari gangguan internal maupun eksternal oleh pihak yang tidak berwenang [8].

Keamanan data RME umumnya ditinjau berdasarkan tiga prinsip utama keamanan informasi, yaitu *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan) yang dikenal sebagai CIA Triad [13]. Prinsip ini menjadi landasan penting dalam merancang pengendalian keamanan pada sistem RME atau SIMRS, dengan tujuan agar hanya pihak yang berwenang dapat mengakses data, data tetap akurat tanpa perubahan tidak sah, serta informasi dapat diakses dengan mudah saat dibutuhkan dalam pelayanan klinis [6].

Berbagai penelitian menunjukkan bahwa implementasi RME masih menghadapi tantangan signifikan terkait keamanan data pasien. Studi pada salah satu rumah sakit di Bandung menemukan kerentanan berupa tidak tersedianya fitur *auto-logout* sehingga sesi pengguna dapat tetap aktif lebih dari enam jam dan meningkatkan risiko akses tidak sah, serta proses pencatatan manual saat terjadi gangguan jaringan yang berpotensi menurunkan akurasi data [6]. Temuan lain menegaskan bahwa kebocoran data pasien dapat menurunkan kepercayaan publik, terutama ketika sistem mengalami *error*, duplikasi data, atau SOP yang belum diperbarui, serta menekankan perlunya integrasi kebijakan, pelatihan sumber daya manusia, dan penguatan kontrol jaringan agar prinsip CIA dapat terimplementasi secara efektif [9]. Penelitian-penelitian tersebut umumnya bersifat literature review atau dilakukan di puskesmas, sedangkan kajian mendalam mengenai keamanan data RME pada aplikasi SIMRS di rumah sakit khusus seperti rumah sakit kepolisian, yang melayani personel POLRI/PNS POLRI beserta keluarganya, masih terbatas.

Kebaruan penelitian ini terletak pada penggambaran secara deskriptif kualitatif terhadap implementasi ketiga aspek CIA Triad secara komprehensif berdasarkan sudut pandang sepuluh informan dari berbagai unit pelayanan, dipadukan dengan hasil observasi, studi dokumentasi, dan triangulasi dengan unit teknologi informasi pada SIMRS RS Bhayangkara Polda DIY. Berdasarkan uraian tersebut, penelitian ini bertujuan untuk menganalisis keamanan data rekam medis elektronik pada aplikasi SIMRS berdasarkan aspek *confidentiality*, *integrity*, dan *availability* di RS Bhayangkara Polda DIY.

2. Metode

2.1 Desain Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan desain studi kasus deskriptif, bertujuan menggambarkan dan menganalisis keamanan data rekam medis elektronik pada aplikasi SIMRS berdasarkan aspek *confidentiality*, *integrity*, dan *availability* di RS Bhayangkara Polda DIY. Pendekatan deskriptif kualitatif digunakan untuk memperoleh pemahaman berdasarkan telaah berbagai sumber dan diperkuat dengan teknik triangulasi sebagai upaya validasi data [14].

2.2 Waktu dan Tempat Penelitian

Penelitian dilaksanakan di Rumah Sakit Bhayangkara Polda DIY, sebuah rumah sakit kepolisian yang berlokasi di Jalan Raya Solo-Yogyakarta Km. 14, Kalasan, Sleman, Daerah Istimewa Yogyakarta, pada periode 10 April-5 Mei 2026.

2.3 Subjek dan Objek Penelitian

Subjek penelitian berjumlah 10 petugas, terdiri atas Kepala Ruang Rekam Medis, Dokter Umum, Dokter Spesialis, Perawat, Kepala Ruang Farmasi, Kepala Ruang Fisioterapi, Kepala Ruang Administrasi/Kasir, Kepala Ruang Radiologi, dan Kepala Ruang Laboratorium, ditambah satu informan triangulasi dari Kepala Ruang IT. Kriteria informan adalah petugas yang menjabat minimal satu tahun (untuk kepala ruang) atau memiliki masa kerja minimal tiga tahun dengan pengalaman menggunakan SIMRS serta memahami hak akses dan keamanan data rekam medis elektronik. Objek penelitian adalah keamanan data RME dan aplikasi SIMRS di RS Bhayangkara Polda DIY.

2.4 Pengumpulan Data

Jenis data yang digunakan meliputi data primer yang diperoleh melalui wawancara mendalam dan observasi, serta data sekunder yang bersumber dari dokumen kebijakan dan SOP rumah sakit. Pengumpulan data dilakukan melalui tiga teknik, yaitu wawancara mendalam menggunakan pedoman wawancara semi-terstruktur, observasi terhadap tampilan dan fitur keamanan SIMRS, serta studi dokumentasi terhadap SOP keamanan data, bukti *backup* data, dan enkripsi data pasien. Wawancara dilaksanakan secara bertahap pada bulan April–Mei 2026 kepada masing-masing informan secara terpisah.

2.5 Keabsahan Data

Keabsahan data diperoleh melalui triangulasi sumber, yaitu membandingkan hasil wawancara antar informan dari berbagai unit pelayanan dengan hasil wawancara informan triangulasi dari unit IT, serta triangulasi teknik dengan membandingkan hasil wawancara, observasi, dan studi dokumentasi. Analisis data dilakukan mengikuti model interaktif Miles, Huberman, dan Saldana, yang terdiri atas tahap kondensasi data, penyajian data, dan penarikan

kesimpulan/verifikasi [10]. Penelitian ini telah memperhatikan etika penelitian, meliputi persetujuan penelitian dari institusi terkait dan kerahasiaan identitas informan.

3. Hasil dan Pembahasan

Penelitian dilaksanakan di RS Bhayangkara Polda DIY, sebuah rumah sakit tipe III milik POLRI yang menyelenggarakan pelayanan kesehatan bagi personel POLRI/PNS POLRI beserta keluarganya serta pelayanan kedokteran kepolisian. Rumah sakit ini telah menerapkan aplikasi SIMRS yang terintegrasi dengan penyelenggaraan rekam medis elektronik pada seluruh unit pelayanan. Informasi diperoleh dari 9 informan utama dan 1 informan triangulasi dari unit IT, dengan rentang usia 33–47 tahun dan latar belakang pendidikan yang bervariasi mulai dari SMK hingga S2.

3.1. Aspek *Confidentiality* (Kerahasiaan)

Hasil penelitian menunjukkan bahwa pengaturan hak akses pengguna SIMRS telah disesuaikan dengan tugas dan tanggung jawab masing-masing petugas. Setiap pengguna memiliki *username* dan *password* pribadi sehingga akses ke data pasien dibatasi sesuai kewenangan dan kebutuhan pelayanan. Sistem *login* SIMRS juga dilengkapi *captcha* sebagai pengamanan tambahan untuk mencegah akses tidak sah, serta fitur *automatic logout* dengan batas waktu sekitar 90 menit yang akan mengakhiri sesi pengguna secara otomatis apabila tidak ada aktivitas. Pengawasan terhadap penggunaan akun dilakukan oleh kepala unit dan tim IT, termasuk pemberian teguran apabila ditemukan praktik penggunaan akun secara bersama (account sharing). Rumah sakit telah memiliki SOP Keamanan dan Perlindungan Data SIMRS secara umum yang telah disosialisasikan kepada seluruh pengguna, meskipun sebagian unit menyatakan belum memiliki SOP kerahasiaan data yang spesifik untuk unitnya.

Penerapan mekanisme Role-Based Access Control (RBAC) melalui kombinasi username dan password sejalan dengan prinsip least privilege, yaitu pemberian hak akses seminimal mungkin sesuai kebutuhan kerja pengguna, sebagaimana dinyatakan bahwa kewenangan yang diberikan sesuai peran dan tanggung jawab dapat diterapkan untuk menjamin aspek confidentiality RME [17]. Penambahan captcha pada halaman login menunjukkan adanya lapisan autentikasi tambahan, sejalan dengan pernyataan bahwa autentikasi berlapis seperti password yang kuat, automatic logout, dan mekanisme verifikasi tambahan diperlukan untuk mengurangi risiko penyalahgunaan akun pada sistem RME [18]. Ketersediaan fitur automatic logout yang berfungsi dengan baik menjadi nilai tambah, mengingat penelitian lain menemukan ketiadaan fitur tersebut sebagai kelemahan utama aspek confidentiality di beberapa puskesmas [6].

Meskipun demikian, masih ditemukan kelemahan berupa praktik account sharing antar petugas dalam pelayanan sehari-hari, yang berpotensi menimbulkan risiko keamanan data karena akuntabilitas pengguna menjadi tidak jelas dan sulit dilacak, sejalan dengan temuan bahwa penggunaan akun bersama masih dilakukan petugas dengan alasan efisiensi pelayanan [8]. Kebijakan penggantian password secara berkala setiap tiga bulan juga belum berjalan optimal karena masih terdapat petugas yang belum mematuhi ketentuan tersebut, padahal penggantian *password* secara berkala merupakan pengamanan dasar yang direkomendasikan untuk melindungi kerahasiaan data pengguna [20]. Keberadaan SOP keamanan data secara umum merupakan langkah maju, namun penerapannya dalam praktik sehari-hari perlu dilakukan secara konsisten, karena keberadaan SOP saja tidak cukup apabila tidak disertai sosialisasi, pemantauan kepatuhan, dan evaluasi berkala [19]. Secara keseluruhan, aspek *confidentiality* pada SIMRS RS Bhayangkara Polda DIY telah didukung oleh mekanisme dasar yang memadai, tetapi pengawasan kepatuhan dan penguatan SOP di tingkat unit masih perlu ditingkatkan.

3.2. Aspek *Integrity* (Integritas)

Pada aspek *integrity*, hasil penelitian menunjukkan bahwa sistem pembatasan kewenangan untuk melakukan perubahan data telah diterapkan, di mana tidak semua pengguna dapat mengubah data secara bebas dan perubahan data yang telah difinalisasi memerlukan koordinasi dengan tim IT. Setiap pengguna pada umumnya hanya dapat mengubah data sesuai akun dan bidang tugasnya, misalnya data medis oleh dokter, data keperawatan oleh perawat, data farmasi

oleh petugas farmasi, dan data administratif oleh petugas pendaftaran. RS Bhayangkara Polda DIY telah menerapkan kebijakan pembatasan waktu revisi data pasien selama tiga hari setelah data diinput, setelah itu sistem akan terkunci *(lock)* sehingga perubahan hanya dapat dilakukan melalui izin IT. Fitur *audit trail* telah tersedia pada SIMRS, namun aksesnya masih terbatas pada petugas IT selaku administrator sistem, dan implementasi tanda tangan elektronik telah diterapkan pada seluruh pengguna yang memiliki kewenangan dalam RME meskipun penggunaannya terus digalakkan untuk dioptimalkan.

Mekanisme pembatasan kewenangan perubahan data sejalan dengan prinsip integritas yang menekankan bahwa perubahan data hanya boleh dilakukan oleh pihak yang berwenang [20], dan merupakan langkah positif dalam menjaga keutuhan data RME. Namun, pembatasan akses fitur *audit trail* hanya kepada petugas IT menyebabkan pemantauan riwayat perubahan data tidak dapat dilakukan secara mandiri oleh pengguna maupun supervisor unit terkait, sehingga transparansi dan akuntabilitas perubahan data menjadi terbatas. Hal ini perlu diperhatikan mengingat jejak audit merupakan rekaman yang mencatat identitas pengakses, jenis perubahan, dan waktu akses yang sangat diperlukan untuk meningkatkan integritas dan keamanan rekam medis pasien [21]. Apabila pembatasan akses tersebut tidak disertai mekanisme monitoring dan pelaporan yang efektif kepada kepala unit, kondisi ini berpotensi menghambat identifikasi dini terhadap potensi manipulasi data.

Implementasi tanda tangan elektronik pada seluruh pengguna yang berwenang turut mendukung keaslian dan keabsahan dokumen elektronik, mengingat integritas data dalam tanda tangan elektronik merujuk pada kondisi data yang tetap utuh dan terlindungi dari perubahan tidak sah setelah proses penandatanganan [22]. Kebijakan pengunci data setelah tiga hari merupakan upaya menjaga integritas data agar terhindar dari perubahan tidak sah pasca finalisasi, namun belum disertai evaluasi berkala terkait integritas data SIMRS yang masih menjadi tantangan dalam pengawasan kualitas dan konsistensi data secara berkelanjutan. Secara umum, aspek *integrity* pada SIMRS RS Bhayangkara Polda DIY telah didukung oleh elemen dasar yang memadai, namun perluasan akses pemantauan *audit trail* dan evaluasi berkala masih diperlukan agar sejalan dengan ketentuan Permenkes RI Nomor 24 Tahun 2022 dan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik.

3.3. Aspek *Availability* (Ketersediaan)

Hasil penelitian pada aspek *availability* menunjukkan kondisi yang relatif lebih baik dibandingkan dua aspek sebelumnya. SIMRS telah terintegrasi antar unit pelayanan secara real-time, sehingga data pasien dapat diakses langsung oleh berbagai unit mulai dari pendaftaran, rawat jalan, rawat inap, farmasi, laboratorium, fisioterapi, hingga radiologi. Tim IT melakukan *backup* data secara otomatis dua kali sehari, yaitu pada sore hari setelah pelayanan selesai dan dini hari sekitar pukul 02.00–03.00 WIB, didukung dengan server *backup* terpisah dan uji restore mingguan, meskipun petugas unit pelayanan umumnya tidak mengetahui jadwal *backup* secara rinci. Rumah sakit juga telah memiliki SOP penanganan *downtime* terencana maupun tidak terencana sebagai pedoman bagi petugas saat terjadi gangguan sistem.

Kendala yang masih ditemukan antara lain gangguan jaringan internet yang menyebabkan SIMRS melambat atau tidak dapat diakses, dengan durasi gangguan ringan kurang dari 30 menit hingga gangguan berat 10–12 jam, serta gangguan pada proses *bridging* data ke sistem eksternal seperti BPJS Klaim, BPJS Antrean, IDRG, dan Satu Sehat yang menghambat proses klaim dan pelaporan data kesehatan nasional. Selain itu, beberapa unit seperti Rekam Medis, Fisioterapi, Farmasi, dan Administrasi/Kasir belum dilengkapi *Uninterruptible Power Supply* (UPS), sehingga data yang sedang diinput berisiko hilang saat terjadi pemadaman listrik mendadak. Pada kondisi gangguan, pelayanan tetap dilakukan secara manual terlebih dahulu kemudian diinput ulang ke SIMRS setelah sistem dapat diakses kembali.

Integrasi SIMRS antar unit pelayanan yang telah berjalan merupakan nilai positif aspek ketersediaan, sejalan dengan pernyataan bahwa integrasi aplikasi SIMRS dengan RME memungkinkan rekam medis pasien terus ter-*update* sejak kunjungan pertama hingga tindak lanjut perawatan, sehingga meningkatkan efisiensi dan kualitas layanan [7]. Kendala bridging data ke sistem eksternal relevan dengan temuan bahwa masalah koneksi dan interoperabilitas dengan sistem eksternal merupakan tantangan ketersediaan pada sistem RME di Indonesia yang memerlukan penanganan sistematis [9]. Pelaksanaan backup data berkala yang didukung

prosedur disaster recovery serta SOP downtime berperan penting dalam meminimalkan risiko kehilangan data, mengingat SOP penanganan *downtime* diperlukan sebagai acuan baku dalam menjaga keberlangsungan pelayanan saat terjadi gangguan sistem informasi [23]. Sementara itu, ketiadaan UPS pada beberapa unit menjadi penyebab utama hilangnya data saat pemadaman listrik mendadak, padahal rekam kesehatan elektronik harus memiliki karakteristik ketersediaan yang tinggi dan mampu menampilkan kembali data yang telah tersimpan sebelumnya [22]. Penyediaan UPS pada setiap titik akses SIMRS perlu segera diprioritaskan untuk mencegah terulangnya kehilangan data.

4. Kesimpulan

Penerapan keamanan data rekam medis elektronik pada aplikasi SIMRS di RS Bhayangkara Polda DIY berdasarkan aspek CIA Triad secara umum telah berjalan namun masih terdapat kekurangan. Pada aspek *confidentiality*, keamanan telah didukung oleh *Role-Based Access Control* melalui *username* dan *password* individual, *captcha*, fitur *automatic logout*, serta SOP Keamanan dan Perlindungan Data SIMRS, tetapi praktik *account sharing* dan kepatuhan penggantian *password* berkala belum sepenuhnya terlaksana. Pada aspek *integrity*, keamanan telah didukung oleh pembatasan hak akses perubahan data, *audit trail*, tanda tangan elektronik, dan pengunci data tiga hari, tetapi akses *audit trail* masih terbatas pada petugas IT dan penggunaan tanda tangan elektronik masih terus dioptimalkan. Pada aspek *availability*, SIMRS telah terintegrasi *real-time* antar unit, didukung *backup* data harian otomatis, server cadangan, serta SOP *downtime*, tetapi masih terdapat kendala *bridging* ke sistem eksternal (BPJS, IDRG, Satu Sehat) dan risiko kehilangan data akibat ketiadaan UPS pada unit Rekam Medis, Fisioterapi, Farmasi, dan Administrasi/Kasir.

Pihak RS Bhayangkara Polda DIY disarankan untuk meningkatkan pengawasan kepatuhan terhadap SOP keamanan data dan larangan *account sharing*, menetapkan kebijakan penggantian *password* secara berkala, serta melengkapi SOP dengan prosedur penanganan insiden keamanan data dan penonaktifan akun pengguna yang berhenti bekerja. Tim IT perlu mengoptimalkan fitur *audit trail* dengan mempertimbangkan akses pemantauan bagi kepala unit, menggalakkan penggunaan tanda tangan elektronik secara konsisten, melaksanakan evaluasi berkala terhadap integritas dan keamanan data SIMRS, menyediakan UPS pada setiap titik akses SIMRS, meningkatkan stabilitas koneksi *bridging* ke sistem eksternal beserta mekanisme alternatifnya, serta melakukan monitoring dan evaluasi rutin terhadap sistem *backup* data. Penelitian selanjutnya disarankan untuk mengembangkan kajian dengan menambahkan aspek *authentication* dan *non-repudiation* guna memperoleh gambaran keamanan data yang lebih komprehensif, serta dilakukan di rumah sakit lain dengan jenis dan tingkat berbeda untuk membandingkan implementasi keamanan data RME lintas institusi.

5. Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada Direktur RS Bhayangkara Polda DIY beserta seluruh staf dan jajaran pelayanan yang telah memberikan izin dan membantu penyediaan data dan informasi selama proses penelitian. Ucapan terima kasih juga disampaikan kepada Politeknik Kesehatan Kementerian Kesehatan Yogyakarta atas dukungan fasilitas dan kesempatan yang diberikan dalam pelaksanaan penelitian ini.

6. Referensi

[1] A. Budiman, M. Isa, dan S. Soekiswati, “Analisis Risiko Dan Tindakan Pencegahan Kebocoran Data Rekam Medis Elektronik Pasien Di RSUP Surakarta,” Jurnal Riset Rumpun Ilmu Ekonomi, vol. 7, no. 3, pp. 2118–2127, 2025.

[2] A. S. Hidayat et al., “Pengaruh Sistem Informasi Kesehatan Terhadap Peningkatan Kualitas Pelayanan Medis Di Puskesmas *(Literature Review)*,” Jurnal Manajemen Informasi Kesehatan, vol. 10, no. 1, pp. 1–10, 2024.

[3] Pemerintah Republik Indonesia, “Undang-Undang Republik Indonesia Nomor 17 Tahun 2023 Tentang Kesehatan,” 2023.

[4] Kementerian Kesehatan Republik Indonesia, "Peraturan Menteri Kesehatan RI Nomor 24 Tahun 2022 tentang Rekam Medis," Peraturan Menteri Kesehatan Republik Indonesia, vol. 151, no. 2, pp. 1–19, 2022.
[5] S. W. Widiyanti *et al.,* "Tinjauan Keamanan Data Rekam Medis Elektronik Pada Aplikasi SIMPUS Berdasarkan Aspek *Confidentiality, Integrity,* Dan *Availability* Di Puskesmas Tasikmadu Karanganyar," *Indonesian Journal of Health Information Management,* vol. 4, no. 2, pp. 1–6, 2024.
[6] S. Ayuni et al., "Implementasi Rekam Medis Elektronik Di Rumah Sakit," Jurnal Kesehatan Albar, vol. 8, no. 1, 2025.
[7] E. Ardianto dan L. Nurjanah, "Analisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik Di Rumah Sakit X," Rekam Medik dan Manajemen Informasi Kesehatan, vol. 3, no. 2, pp. 18–30, 2024.
[8] D. Wijayanti *et al., "Uncovering Security Vulnerabilities In Electronic Medical Record Systems: A Comprehensive Review Of Threats And Recommendations For Enhancement,*" Jurnal Ilmiah Teknik Elektro Komputer dan Informatika, vol. 10, no. 1, pp. 73–98, 2024.
[9] Miles, A. M. Hubberman, dan J. Saldana, *Qualitative Data Analysis: A Methods Sourcebook, 4th ed. Thousand Oaks, CA: SAGE Publications, 2019.*
[10] A. H. Harahap *et al.,* "Pentingnya Peranan CIA Triad Dalam Keamanan Informasi Dan Data Untuk Pemangku Kepentingan Atau Stakeholder," Jurnal Manajemen Pendidikan dan Ilmu Sosial, vol. 1, no. 2, pp. 73–83, 2023.
[11] S. Qadir dan S. M. K. Quadri*, "Information Availability: An Insight Into The Most Important Attribute Of Information Security," Journal of Information Security*, pp. 185–194, 2016.
[12] M. Waruwu, "Pendekatan Penelitian Kualitatif: Konsep, Prosedur, Kelebihan Dan Peran Di Bidang Pendidikan," vol. 5, pp. 198–211, 2024.
[13] L. Judijanto et al., Analisis dan Perancangan Sistem Informasi Kesehatan. Bandung: CV. Selembar Karya Pustaka, 2024.
[14] W. Mulyani, D. L. S. Kurniasih, dan A. Sukawan, "Hak Akses Pelepasan Informasi Rekam Medis Elektronik Untuk Kepentingan Penelitian Di RSUP Dr. Hasan Sadikin Bandung," Jurnal Kebijakan Kesehatan Indonesia: JKKI, vol. 12, no. 3, pp. 154–159, 2023.
[15] F. R. Ikawati, A. Ansyori, dan D. A. S. Permatasari, *"Literature Review:* Analisis Keamanan Data Rekam Medis Elektronik di Fasilitas Kesehatan," Jurnal Manajemen Informasi Kesehatan, vol. 10, no. 2, pp. 230–237, 2025.
[16] L. Prabawati, F. R. Ikawati, dan L. Afifah, "Tinjauan Keamanan Data Rekam Medis Elektronik Di Puskesmas Jabung," Jurnal Vokasi Kesehatan, vol. 4, no. 1, pp. 87–94, 2025.
[17] E. Wardani *et al.,* "Keamanan Sistem Informasi Rekam Medis Elektronik Di Rumah Sakit Islam Jakarta Sukapura," Rekam Medik dan Manajemen Informasi Kesehatan, vol. 3, no. 2, pp. 31–38, 2024.
[18] H. Meilani, S. W. Nugraheni, dan B. Suprawita, "Analisis Implementasi Rekam Medis Elektronik Terhadap Mutu Pelayanan Rawat Jalan Di RSUD Ibu Fatmawati Soekarno Kota Surakarta," vol. 15, no. 2, pp. 158–164, 2025.
[19] S. Sofia, E. T. Ardianto, dan N. Muna, "Analisis Aspek Keamanan Informasi Pasien Pada Penerapan RME Di Fasilitas Kesehatan," Rekam Medik dan Manajemen Informasi Kesehatan, vol. 1, no. 2, pp. 94–103, 2022.
[20] A. Wiwaha dan A. Ulfah, "Tinjauan Penanganan Downtime di Pendaftaran Rawat Jalan Guna Menunjang Akreditasi Versi Starkes," Prepotif: Jurnal Kesehatan Masyarakat, vol. 8, no. 2, pp. 2951–2957, 2024.
[21] P. W. Handayani *et al.,* Pengantar Sistem Informasi Manajemen Rumah Sakit (SIMRS). Jakarta: Rajawali Pers, 2018.
[22] A. Rukmana *et al.,* Pengantar Sistem Informasi: Panduan Praktis Pengenalan Sistem Informasi dan Penerapannya. Bandung: PT Sonpedia Publishing Indonesia, 2023.