BAB I

PENDAHULUAN

A. Latar Belakang

Di era globalisasi saat ini, kemajuan teknologi berkembang pesat, dan salah satunya adalah perkembangan Teknologi Informasi (TI). Teknologi informasi telah diterapkan di berbagai bidang, termasuk bidang kesehatan. Salah satu penerapan teknologi ini adalah Rekam Medis Elektronik (RME) pada Sistem Informasi Manajemen Rumah Sakit (SIMRS) yang merupakan solusi TI untuk mengumpulkan, menyimpan, memproses, dan mengakses data yang tersimpan dalam sistem manajemen basis data (Budiman, Isa dan Soekiswati, 2025). Dengan penggunaan sistem informasi dalam layanan kesehatan dapat memberikan banyak manfaat bagi penyedia layanan kesehatan, seperti meningkatkan mutu pelayanan, mengurangi kesalahan medis, meningkatkan pemahaman tentang ketersediaan fasilitas dan akses informasi, dan meningkatkan kualitas pengambilan keputusan berbasis data (Hidayat *et al.*, 2025).

Rumah sakit sebagai fasilitas pelayanan kesehatan yang menyelenggarakan pelayanan kesehatan perseorangan secara paripurna melalui pelayanan kesehatan promotif, preventif, kuratif, rehabilitatif, dan/atau paliatif dengan menyediakan pelayanan rawat inap, rawat jalan, dan gawat darurat (UU No. 17, 2023). Rumah sakit memiliki kewajiban untuk menyelenggarakan rekam medis elektronik yang mencatat data pasien

secara terus-menerus, sejak pasien datang hingga dipulangkan (Sheviyana *et al*., 2020).

Penyelenggaraan Rekam Medis Elektronik (RME) berdasarkan Permenkes RI No. 24 Tahun 2022 yaitu mewajibkan Fasilitas Pelayanan Kesehatan (Fasyankes), termasuk rumah sakit dan puskesmas, untuk menerapkan RME paling lambat 31 Desember 2023 (Permenkes RI No. 24, 2022). Tujuan utama dari rekam medis elektronik adalah untuk peningkatan dalam penyimpanan, pemrosesan, dan pertukaran informasi kesehatan, yang pada akhirnya dapat meningkatkan kualitas pelayanan kesehatan secara keseluruhan, serta untuk memenuhi prinsip keamanan dan kerahasiaan data informasi medis pasien (Widiyanti *et al.*, 2024).

Salah satu penerapan penting RME adalah melalui Sistem Informasi Manajemen Rumah Sakit (SIMRS), yang memungkinkan pendaftaran pasien dilakukan secara elektronik guna memudahkan pengelolaan data secara *real-time* dan akurat. Integrasi aplikasi SIMRS dengan RME memungkinkan rekam medis pasien terus terupdate sejak kunjungan pertama hingga tindak lanjut perawatan, meningkatkan efisiensi dan kualitas layanan (Ayuni *et al.*, 2025). Dalam pengelolaan rekam medis elektronik, prinsip-prinsip keamanan data dan informasi, termasuk kerahasiaan, integritas, dan ketersediaan, harus diperhatikan untuk memastikan keamanan data dan informasi dalam rekam medis elektronik serta perlindungannya terhadap gangguan internal dan eksternal oleh pihak yang tidak berwenang (Ardianto dan Nurjanah, 2024).

Menurut Permenkes RI Nomor 24 Tahun 2022 tentang Rekam Medis telah mengatur terkait dengan keamanan RME dimana rekam medis diselenggarakan secara elektronik dengan tujuan menjamin keamanan, kerahasiaan, keutuhan, dan ketersediaan (Permenkes RI No. 24, 2022). Keamanan data RME biasanya ditinjau berdasarkan tiga prinsip utama dalam keamanan informasi, yaitu *Confidentiality* (kerahasiaan), *Integrity* (keutuhan), dan *Availability* (ketersediaan) yang dikenal sebagai CIA Triad. Prinsip ini menjadi landasan penting dalam merancang pengendalian keamanan pada sistem EMR atau SIMRS, dengan tujuan agar hanya pihak yang berwenang yang dapat mengakses data, data tetap terjaga keasliannya tanpa perubahan yang tidak sah, dan informasi dapat diakses dengan mudah saat dibutuhkan dalam proses pelayanan klinis (Wijayanti *et al.*, 2024).

Berbagai penelitian menunjukkan bahwa implementasi RME masih menghadapi tantangan signifikan terkait keamanan data pasien. Studi di salah satu rumah sakit di Bandung menemukan adanya kerentanan seperti tidak tersedianya fitur *auto-logout* sehingga sesi pengguna dapat tetap aktif lebih dari enam jam dan meningkatkan risiko akses tidak sah. Selain itu, ketika terjadi gangguan jaringan, proses pencatatan kembali dilakukan secara manual yang berpotensi menurunkan akurasi dan efisiensi pengelolaan data. Temuan lain menegaskan bahwa kebocoran data pasien dapat menyebabkan kerugian material maupun non-material serta menurunkan kepercayaan publik, terutama ketika sistem mengalami *error,* data ganda, atau SOP belum diperbarui. Studi tinjauan pada konteks

Indonesia juga menekankan perlunya integrasi kebijakan, pelatihan SDM, dan penguatan kontrol jaringan agar prinsip CIA dapat terimplementasi efektif. Temuan ini menunjukkan bahwa isu-isu keamanan EMR bukan hanya masalah teknologi, tetapi juga manajemen risiko dan kesiapan sumber daya manusia (Wijayanti *et al.*, 2024).

Berdasarkan studi pendahuluan melalui wawancara pada tanggal 24 November 2025 di Ruang Binfung dengan Kepala Ruang Rekam Medis RS Bhayangkara Polda DIY, diketahui bahwa RS Bhayangkara Polda DIY telah menyelenggarakan SIMRS sejak tahun 2011 bernama Sistem Informasi Manajemen Rumah Sakit Bhayangkara Polda DIY dalam bentuk aplikasi berbasis website. Keamanan data pada SIMRS berdasarkan aspek *confidentiality,* dalam pelayanan sehari-hari masih sering terjadi penggunaan akun secara bersama atau pinjam-meminjam akun untuk mengakses Aplikasi SIMRS dengan tujuan mempercepat proses pelayanan. Pada Aplikasi SIMRS sudah dilengkapi dengan *automatic logout* apabila SIMRS tidak digunakan dalam beberapa waktu. Di RS Bhayangkara Polda DIY diketahui belum terdapat Standar Operasional Prosedur (SOP) yang secara khusus mengatur penyelenggaraan RME, terutama yang membahas aspek keamanan informasi rekam medis pada Aplikasi SIMRS.

Pada aspek *integrity*, SIMRS di RS Bhayangkara Polda DIY belum terdapat fasilitas tanda tangan elektronik. RS Bhayangkara Polda DIY belum pernah melakukan evaluasi terkait keamanan data pada Aplikasi SIMRS. Pada aspek *availability,* SIMRS sudah saling terintegrasi antar unit

pelayanan. Namun, masih ditemukan kendala yaitu terkadang SIMRS mengalami *error* pada *bridging* data ke BPJS Klaim, BPJS Antrean, *Indonesian Diagnosis Related Group* (IDRG), dan Satu Sehat. Dalam Aplikasi SIMRS, pada perangkat keras belum tersedia *Universal Serial Bus* (USB) dan media eksternal lainnya. Akibatnya, ketika terjadi pemadaman listrik, data yang sedang diinput langsung hilang dan petugas harus menginputkannya lagi. Dari uraian latar belakang permasalahan tersebut, peneliti akan melakukan penelitian lebih lanjut untuk mengkaji secara mendalam mengenai "Gambaran Keamanan Data pada Aplikasi SIMRS Berdasarkan Aspek CIA Triad di RS Bhayangkara Polda DIY".

B. Rumusan Masalah

Berdasarkan uraian latar belakang masalah yang telah diuraikan tersebut, maka dapat dirumuskan permasalahan terkait "Bagaimana Tinjauan Keamanan Data Rekam Medis Elektronik Pada Aplikasi SIMRS Berdasarkan Aspek CIA Triad di Rumah Sakit Bhayangkara Polda DIY?"

C. Tujuan Penelitian

1. Tujuan Umum

   Menggambarkan keamanan data rekam medis elektronik pada Aplikasi SIMRS berdasarkan Aspek CIA Triad di Rumah Sakit Bhayangkara Polda DIY.

2. Tujuan Khusus:

   a. Menggambarkan keamanan data RME pada aplikasi SIMRS berdasarkan aspek kerahasiaan *(confidentiality)* di RS Bhayangkara Polda DIY.
   b. Menggambarkan keamanan data RME pada aplikasi SIMRS berdasarkan aspek integritas *(integrity)* di RS Bhayangkara Polda DIY.
   c. Menggambarkan keamanan data RME pada aplikasi SIMRS berdasarkan aspek ketersediaan *(availability)* di RS Bhayangkara Polda DIY.

D. Ruang Lingkup

Ruang lingkup penelitian ini adalah sebagai berikut:

1. Ruang Lingkup Waktu

   Penelitian ini dilaksanakan pada tanggal 10 April hingga 5 Mei 2026.

2. Ruang Lingkup Lokasi

   Penelitian ini dilaksanakan di Ruang Rekam Medis, Ruang Teknologi Informasi, dan Rumah Sakit Bhayangkara Polda DIY yang beralamat di Jalan Raya Solo-Yogyakarta KM.14, Dusun Glondong, Kelurahan Tirtomartani, Kecamatan Kalasan, Kabupaten Sleman, Daerah Istimewa Yogyakarta, 55571.

3. Ruang Lingkup Materi

   Membahas tentang Analisis Keamanan Data Rekam Medis Elektronik.

E. Manfaat Penelitian

1. Manfaat Teoritis:

   a. Memberikan kontribusi pengetahuan terkait keamanan data rekam medis elektronik, khususnya aspek *confidentiality, integrity,* dan *availability* dalam aplikasi SIMRS.

   b. Menambah wawasan akademik tentang penerapan teknologi informasi dalam pelayanan kesehatan secara aman dan terstandarisasi.

   c. Menjadi referensi bagi pengembangan studi lanjutan mengenai keamanan data dalam sistem rekam medis elektronik di institusi kesehatan.

2. Manfaat Praktis:

   a. Bagi Mahasiswa:

      1) Sebagai bahan pembelajaran dan peningkatan pemahaman mengenai aspek keamanan data rekam medis elektronik dalam sistem informasi rumah sakit.

      2) Membantu mahasiswa mengaplikasikan teori keamanan informasi dalam pelayanan kesehatan dan pengembangan penelitian terkait TI kesehatan.

b. Bagi Rumah Sakit:

1) Memberikan evaluasi dan gambaran nyata tentang efektivitas penerapan keamanan data pada aplikasi SIMRS.
2) Menjadi dasar rekomendasi perbaikan kebijakan dan prosedur keamanan data rekam medis elektronik untuk meningkatkan perlindungan data pasien.
3) Mendukung upaya rumah sakit dalam memastikan keamanan, kerahasiaan, dan ketersediaan data sebagai bagian dari peningkatan mutu pelayanan kesehatan berbasis teknologi.

c. Bagi Peneliti:

Penelitian ini memberikan kesempatan dalam meningkatkan pemahaman mendalam mengenai konsep dan penerapan keamanan data rekam medis elektronik berdasarkan kerangka CIA Triad, sekaligus mengembangkan kemampuan analisis kritis terhadap efektivitas kontrol keamanan pada Aplikasi SIMRS di RS Bhayangkara Polda DIY.

F. Keaslian Penelitian

Penelitian terkait Tinjauan Keamanan Data Rekam Medis Elektronik Pada Aplikasi SIMRS Berdasarkan Aspek CIA Triad di Rumah Sakit Bhayangkara Polda DIY belum pernah dilakukan sebelumnya. Berikut ini beberapa penelitian yang hampir serupa dan pernah dilakukan, antara lain:

Tabel 1. Keaslian Penelitian.

No.	Judul dan Nama Peneliti	Metode Penelitian	Hasil Penelitian	Persamaan dan Perbedaan
1.	Keamanan Data Rekam Medis Elektronik Menggunakan Teknik Kriptografi: *Literature Review* (Vira-Febriyana dan Ichwani, 2023)	*Literature Review* pada 15 artikel jurnal terpilih.	Teknik kriptografi mampu melindungi keamanan data rekam medis elektronik dengan tingkat keamanan tinggi berdasarkan kompleksitas kunci yang digunakan.	**Persamaan:** Fokus pada keamanan data rekam medis dengan aspek *confidentiality, integrity, dan availability.* **Perbedaan:** Menggunakan metode *literature review,* sedangkan penelitian ini menggunakan kualitatif deskriptif.
2.	Analisis Keamanan Data Pasien Dalam Rekam Medis Elektronik Berdasarkan Cia Triad Di RSUD X Jawa Tengah (Setyaningrum dan Ricky, 2025).	Deskriptif dengan pendekatan kualitatif.	Aspek *Confidentiality* masih lemah karena 60% petugas menggunakan *password* sederhana dan belum ada MFA; *Integrity* belum optimal akibat *audit trail* hanya tercatat pada level database; *Availability* relatif baik (*uptime* 98,5%) namun RTO masih 8–12 jam dan server melambat di atas 1.500 request/jam.	**Persamaan:** Meneliti keamanan RME menggunakan aspek CIA Triad *(confidentiality, integrity, availability).* **Perbedaan:** Penelitian tersebut fokus pada fenomena keamanan data pasien pada RME di RSUD X, sedangkan penelitian ini fokus pada Aplikasi SIMRS.

No.	Judul dan Nama Peneliti	Metode Penelitian	Hasil Penelitian	Persamaan dan Perbedaan
3.	Analisis Aspek Keamanan Data Pasien dalam Implementasi RME di RS X (Ardianto dan Nurjanah, 2024)	Kualitatif: Wawancara, observasi, dokumen.	Keamanan RME: login *username/ password*, edit terbatas, tanda tangan elektronik, akses hanya di RS, belum ada SOP khusus keamanan.	**Persamaan:** Menggunakan analisis CIA dalam RME dan kendala praktik keamanan. **Perbedaan:** Penelitian tersebut umum pada implementasi RME, sedangkan penelitian ini fokus pada keamanan dan aplikasi SIMRS secara spesifik.
4.	Tinjauan Keamanan Data Rekam Medis Elektronik di Puskesmas Jabung (Prabawati, Ikawati and Afifah, 2025).	Kualitatif dengan Pendekatan Studi Kasus.	Kelemahan pada aspek *Confidentiality* (belum ada *log out* otomatis).	**Persamaan:** Menggunakan metode kualitatif dan meninjau keamanan RME berdasarkan aspek CIA. **Perbedaan:** Meninjau keamanan data RME secara keseluruhan yang diterapkan puskesmas, sedangkan penelitian ini hanya berfokus pada Aplikasi SIMRS.
5.	Tinjauan Keamanan Data Rekam Medis Elektronik Pada Aplikasi Simpus Berdasarkan Aspek CIA di Puskesmas Tasikmadu (Widiyanti,	Deskriptif Kualitatif.	Terdapat kelemahan pada *Confidentiality* (belum ada *Automatic Log Off*).	**Persamaan:** Menggunakan metode Kualitatif Deskriptif dan meninjau keamanan RME berdasarkan aspek CIA.

No.	Judul dan Nama Peneliti	Metode Penelitian	Hasil Penelitian	Persamaan dan Perbedaan
	Hastuti, dan Kusumawati, 2024).			**Perbedaan:** Penelitian ini di Puskesmas dan aplikasi SIMPUS, sementara penelitian ini di Rumah Sakit dengan fokus pada Aplikasi SIMRS
6.	Perlindungan Hukum terhadap Privasi Data Pasien dalam Sistem Rekam Medis Elektronik (Herisasono, 2024).	Penelitian Artikel (Fokus Hukum/ Regulasi)	Perlindungan hukum data pasien belum optimal karena implementasi regulasi yang belum merata.	**Persamaan:** Membahas perlindungan data pasien dalam RME. **Perbedaan:** Penelitian ini fokus hukum, sedangkan penelitian saya fokus pada keamanan data dan operasional berdasarkan standar CIA.