BAB I
PENDAHULUAN

A. Latar Belakang

Pesatnya kemajuan teknologi informasi menciptakan perubahan yang cukup signifikan dalam pelayanan kesehatan, sehingga pelayanan harus mampu beradaptasi dan melakukan perubahan. Peraturan Kementrian Kesehatan No. 82 tahun 2013 tentang Sistem Informasi Manajemen Rumah Sakit menyebutkan bahwa setiap Rumah Sakit wajib menyelenggarakan Sistem Informasi Manajemen Rumah Sakit (SIMRS) sebagai suatu sistem komunikasi yang memproses dan mengintegrasikan seluruh alur proses pelayanan Rumah Sakit dalam bentuk jaringan koordinasi, pelaporan dan prosedur administrasi untuk memperoleh informasi secara tepat dan akurat dan merupakan bagian dari Sistem Informasi Kesehatan (Kemenkes RI, 2013).

SIMRS harus memiliki akses keamanan dalam pengelolaannya untuk melindungi data pasien yang bersifat pribadi dan menjaga rekam medis pasien yang bersifat rahasia dan harus dilindungi agar tidak hilang atau bocor, karena hal tersebut dapat mengganggu pelayanan dan perawatan pasien (Christin et al., 2025). Peraturan Menteri Kesehatan No. 24 tahun 2022 tentang Rekam Medis Elektronik mengatur bahwa rekam medis elektronik tidak hanya dituntut efektif dan efisien, tetapi harus memenuhi prinsip keamanan data dan informasi pasien.

Standar keamanan informasi internasional yang diakui adalah ISO/IEC 27001:2022 sebagai pemenuhan persyaratan mengenai kepatuhan dalam peraturan keamanan data. ISO/IEC 27001:2022 memberikan panduan bagi suatu organisasi untuk menetapkan, menerapkan, memelihara dan meningkatkan sistem manajemen keamanan informasi (Aristianto et al., 2025).

Meskipun berbagai standar keamanan sudah tersedia, fenomena kebocoran data masih sering terjadi baik di tingkat internasional maupun

nasional. Di luar negeri, pada tahun 2021 sebanyak 686 pelanggaran data kesehatan yang tercatat oleh Kantor Hak Sipil Departemen Kesehatan Amerika Serikat. Sekitar 44,9 juta data pasien dicuri dan terakses tanpa izin, dengan 73,9% diantaranya disebabkan karena peretasan atau gangguan TI (Alder, 2021).

Kasus kebocoran data banyak terjadi juga di dalam negeri, bukan hanya satu kali kejadian, tetapi kasus kebocoran dan pencurian data kesehatan yang tercatat semakin banyak menunjukkan adanya masalah yang serius dalam hal keamanan data di Indonesia. Pada bulan Mei 2021 diketahui kasus kebocoran data yang cukup besar yang diduga terjadi akibat kelalaian internal dan serangan siber yang berhasil mengambil celah dari kerentanan pada sistem (Singgih, 2025).

Adapun kasus pencurian data kesehatan pada bulan Juni 2020, yaitu kebocoran data pribadi dengan dugaan awal karena lemahnya sistem pencatatan dan pelaporan data (Anggraini, 2023). Salah satu kasus besar yang terjadi di Indonesia yaitu kebocoran data yang dikonfirmasi langsung oleh tim *Cyber Threat Intelligence* Badan Siber dan Sandi Negara (BSSN) yang melaporkan karena adanya replikasi data dari server utama ke server replikasi database untuk backup tanpa adanya standar keamanan yang memadai, dan kurangnya audit keamanan dan pengujian yang tidak rutin dilakukan (Singgih, 2025). Kasus-kasus ini menunjukkan pentingnya kesiapan sistem informasi dalam menghadapi beberapa serangan siber dan meningkatkan keamanan data kesehatan.

Bentuk adaptasi nasional terhadap standar internasional, di Indonesia Badan Siber dan Sandi Negara (BSSN) mengembangkan Indeks Keamanan Informasi (Indeks KAMI) yang digunakan untuk mengetahui gambaran kelengkapan dan kematangan kerangka kerja keamanan informasi berdasarkan standar ISO/IEC 27001:2022. Hasil evaluasi ini menjadi dasar penyusunan langkah perbaikan serta penetapan prioritas dalam peningkatan keamanan informasi (BSSN, 2023).

Sejumlah penelitian sebelumnya telah menggunakan Indeks KAMI sebagai instrumen untuk menilai tingkat keamanan informasi. Misalnya, penelitian oleh Wibawa et al., (2024) menunjukkan belum memenuhi syarat kesiapan dan kematangan untuk standar keamanan data Rumah Sakit. Selain itu, terdapat penelitian oleh Suroso & Wasilah, (2025) menunjukkan bahwa tingkat kesiapan keamanan informasi yang cukup baik, Namun, ada beberapa area yang masih perlu diperbaiki agar keamanan informasi secara keseluruhan bisa lebih baik.

Belum terpenuhinya tingkat kesiapan keamanan data dapat menjadi ancaman terhadap keamanan informasi kesehatan. Data kesehatan yang bersifat rahasia dan sangat sensitif berpotensi mengalami kebocoran atau penyalahgunaan yang dapat mengakibatkan dampak negatif, baik bagi perorangan atau terhadap fasilitas kesehatan (Ahmad et al., 2025).

Berdasarkan hasil studi pendahuluan, RSU Prasetya Bunda Kota Tasikmalaya telah menerapkan SIMRS secara elektronik di seluruh unit pelayanan hingga penunjang medis, sehingga pengelolaan data pasien sangat bergantung pada keandalan sistem informasi. Rumah sakit memang telah memiliki beberapa kebijakan dasar terkait keamanan data, seperti struktur organisasi teknologi informasi dan prosedur kerahasiaan data pasien, namun hingga saat ini belum pernah dilakukan penilaian tingkat kesiapan keamanan sistem elektronik secara menyeluruh.

Kondisi ini menunjukkan adanya ketidaksesuaian dengan ketentuan regulasi, karena Peraturan Pemerintah No. 71 Tahun 2019 mewajibkan setiap Penyelenggara Sistem Elektronik (PSE) untuk menilai, mengendalikan, dan membuktikan kesiapan keamanan sistem elektronik yang digunakan agar dapat dipastikan andal, aman dan bertanggung jawab. Tanpa adanya penilaian yang terukur, rumah sakit tidak dapat memastikan penerapan keamanan informasi yang berjalan telah memenuhi standar dan mampu melindungi data pasien yang bersifat pribadi dan sensitif. Penelitian Daniswara et al., (2023) menegaskan bahwa evaluasi berkala terhadap

prosedur keamanan merupakan langkah penting untuk meningkatkan ketahanan sistem terhadap jenis pelanggaran data.

Jenis pelanggaran data disebutkan pada penelitian (Pool et al., 2024) yaitu pencurian data, kehilangan, dan pembuangan data yang tidak sah. Beberapa pelanggaran tersebut dapat menjadikan konsekuensi sosial dan operasional yang serius karena kepercayaan pasien terhadap rumah sakit menurun, sehingga dapat mempengaruhi pemberian informasi klinis secara lengkap dan menghambat proses layanan kesehatan.

Ketentuan tersebut diperlukan adanya instrumen penilaian yang terstandar dan terukur, sehingga dilakukan penilaian kesiapan keamanan data menggunakan Indeks KAMI yang merupakan instrumen resmi pemerintah dari BSSN yang dirancang untuk menilai kelengkapan dan kematangan penerapan keamanan informasi pada penyelenggara sistem elektronik termasuk rumah sakit.

B. Rumusan Masalah

Bagaimana tingkat kesiapan keamanan informasi di RSU Prasetya Bunda berdasarkan hasil penilaian menggunakan Indeks KAMI 5.0?

C. Tujuan Penelitian

1. Tujuan Umum

   Mengetahui tingkat kesiapan keamanan informasi di RSU Prasetya Bunda menggunakan Indeks KAMI versi 5.0.

2. Tujuan Khusus
   a. Mengetahui alur prosedur pelaksanaan keamanan informasi pada penyelenggaraan SIMRS;
   b. Mengetahui gambaran kelengkapan kontrol dan kematangan penerapan keamanan informasi berdasarkan Indeks KAMI 5.0;
   c. Menganalisis hasil tingkat kesiapan keamanan informasi untuk menggambarkan kondisi kesiapan keamanan informasi.

D. Manfaat Penelitian

Penelitian ini diharapkan bisa memberikan manfaat baik dari segi teori maupun praktis. Berikut ini beberapa manfaat yang bisa diperoleh dari penelitian ini:

1. Manfaat Teoritis
   a. Bagi akademik

      Penelitian ini diharapkan menjadi bahan kajian akademik dalam bidang keamanan informasi untuk mengetahui tingkat kesiapan keamanan pada sistem elektronik yang digunakan di sektor kesehatan, khususnya terkait keamanan pada Sistem Informasi Manajemen Rumah Sakit di RSU Prasetya Bunda Kota Tasikmalaya.

   b. Bagi peneliti

      Penelitian ini diharapkan menjadi pengalaman empiris bagi peneliti dalam mengkaji aspek keamanan informasi dan tata kelola di Rumah Sakit. Selain itu, dapat meningkatkan kemampuan analisis peneliti dalam melakukan evaluasi sistem informasi berbasis standar nasional dan internasional.

2. Manfaat Praktis
   a. Bagi Fasilitas Pelayanan Kesehatan

      Penelitian ini diharapkan membantu Rumah Sakit mengevaluasi tingkat kesiapan dan kematangan keamanan data Sistem Informasi Manajemen Rumah Sakit. Hasil penilaian dapat digunakan sebagai bahan pertimbangan dalam kebijakan dan strategi peningkatan keamanan data pasien.

   b. Bagi pengelola dan pengguna Sistem Informasi Manajemen Rumah Sakit (SIMRS)

      Penelitian ini diharapkan dapat meningkatkan kesadaran petugas dan pengelola SIMRS terdapat pentingnya penerapan keamanan informasi dalam pengelolaan rekam medis elektronik dan menjadi acuan dalam pengawasan akses data pasien secara lebih tepat.

E. Keaslian Penelitian

Tabel 1. 1 Keaslian Penelitian

No	Peneliti	Judul Penelitian	Persamaan	Perbedaan
1.	(Wibawa et al., 2024) *Journal of Information Systems and Informatics*, *6*(4), 3070–3086. https://doi.org/10.51519/journalisi.v6i4.949	*Information Security Evaluation at Hospital Using Index KAMI 5.0 and Recommendations Based on ISO/IEC 27001:2022*	Penelitian sama-sama menggunakan Indeks KAMI 5.0 dalam konteks Rumah Sakit untuk menilai tingkat kesiapan keamanan data.	Penelitian (Wibawa et al., 2024) dilakukan setelah adanya serangan *ransomware* sedangkan penelitian ini bersifat preventif untuk identifikasi kelemahan.
2.	(Jelita et al., 2024) *Jurnal Saintekom*, *14*(1), 84–94. https://doi.org/10.33020/saintekom.v14i1.623	Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/EIC 27001:2022	Penelitian menggunakan Indeks KAMI versi 5.0 yang	Objek penelitian bukan Rumah Sakit, melainkan instansi pendidikan. sedangkan penelitian penulis berfokus pada keamanan data di Rumah Sakit.

No	Peneliti	Judul Penelitian	Persamaan	Perbedaan
3.	(Suroso & Wasilah, 2025) *Teknika*, *19*(x), 795–808. https://jurnal.polsri.ac.id/index.php/teknika/article/view/10705	Analisis Keamanan Informasi SIMRS dengan Metode Indeks KAMI dan OCTAVE Allegro	Penelitian mengevaluasi keamanan informasi pada Sistem Informasi Manajemen Rumah Sakit (SIMRS) menggunakan Indeks KAMI.	Penelitian ini menggunakan versi 4.2 dan dikombinasikan dengan metode OCTAVE Allegro. Sementara penelitian penulis menggunakan Indeks KAMI 5.0.
4.	(Maraqonitatilla & Palupi Ghea Sekar, 2024) *Journal of Emerging Information Systems and Business Intelligence*, *5*(2), 66–72. https://ejournal.unesa.ac.id/index.php/JEISBI/article/view/59469	Analisis Tingkat Keamanan Informasi Pada RSUD Dr. R. Sosodoro Djatikoesoemo Bojonegoro Menggunakan Indeks KAMI Berdasarkan ISO 27001:2013	Penelitian menggunakan Indeks KAMI 5.0 dalam konteks Rumah Sakit untuk menilai tingkat kesiapan dan kematangan keamanan data.	Penelitian menggunakan Indeks KAMI versi 4.2 dengan acuan ISO 27001:2013, sedangkan penelitian ini menggunakan versi terbaru (5.0) yang mengacu pada ISO 27001:2022.