BAB II

TINJAUAN PUSTAKA

A. Telaah Pustaka

1. Rumah Sakit

   a. Pengertian Rumah Sakit

      Rumah sakit merupakan fasilitas pelayanan kesehatan yang menyelenggarakan pelayanan kesehatan perorangan secara menyeluruh melalui pelayanan promotif, preventif, kuratif, dan rehabilitatif. Rumah Sakit menjalankan fungsi pelayanan medis, pelayanan keperawatan, pelayanan penunjang medis, serta fungsi manajerial yang mencakup pengelolaan sumber daya, administrasi, dan sistem informasi kesehatan. Pelaksanaan fungsi tersebut menjadikan rumah sakit sebagai organisasi yang menghasilkan dan mengelola data kesehatan pasien secara berkelanjutan (UU RI No.17, 2023).

   b. Klasifikasi Rumah Sakit Umum

      Rumah sakit umum merupakan fasilitas pelayanan kesehatan yang menyelenggarakan pelayanan kesehatan pada seluruh bidang dan berbagai jenis penyakit. Pelayanan yang diberikan oleh rumah sakit umum tersebut sekurang-kurangnya meliputi pelayanan medik, pelayanan penunjang medik, pelayanan keperawatan dan kebidanan, serta pelayanan nonmedik (Permenkes RI No. 3, 2020). Berikut ini klasifikasi rumah sakit umum yang terdiri atas:

1) Rumah sakit umum kelas A adalah rumah sakit umum yang memiliki jumlah tempat tidur paling sedikit 250 buah.
2) Rumah sakit umum kelas B adalah rumah sakit umum yang memiliki jumlah tempat tidur paling sedikit 200 buah.
3) Rumah sakit umum kelas C adalah rumah sakit umum yang memiliki jumlah tempat tidur paling sedikit 100 buah.
4) Rumah sakit umum kelas D yang memiliki jumlah tempat tidur paling sedikit 50 buah.

2. Rekam Medis Elektronik

a. Pengertian Rekam Medis Elektronik

Rekam Medis Elektronik adalah rekam medis yang dibuat dengan menggunakan sistem elektronik yang diperuntukkan bagi penyelenggaraan rekam medis, RME menjadi dokumen resmi yang ditata secara digital sejak pasien masuk hingga pulang atau dirujuk (Permenkes RI No. 24, 2022). Kemajuan teknologi informasi, khususnya di bidang kesehatan, mendorong perubahan dalam sistem manajemen informasi kesehatan, termasuk peralihan pengelolaan rekam medis dari bentuk manual menuju RME (Ayuni et al. 2025).

b. Unit Rekam Medis.

Unit rekam medis di rumah sakit berperan penting dalam penyelenggaraan rekam medis elektronik sebagai bagian dari sistem informasi kesehatan. Unit ini bertanggung jawab terhadap berbagai kegiatan pengelolaan rekam medis yang meliputi registrasi pasien,

pendistribusian data rekam medis, pengolahan informasi rekam medis, penyimpanan rekam medis, penjaminan mutu, serta transfer isi rekam medis. Melalui pelaksanaan fungsi tersebut, unit rekam medis mendukung pengelolaan informasi kesehatan dan penyelenggaraan sistem informasi pelayanan kesehatan yang terintegrasi di rumah sakit (Permenkes RI No.24, 2022).

Secara operasional, unit rekam medis bertanggung jawab atas berbagai tahapan pengelolaan dokumen yang mencakup pencatatan (registrasi) informasi pasien, pengolahan data, serta penyimpanan berkas rekam medis secara sistematis. Aktivitas ini meliputi proses *assembling*, *coding*, *indexing*, *analyzing*, *reporting*, dan *filing* yang memastikan bahwa informasi kesehatan tersaji dengan lengkap, mudah diakses. Peran unit rekam medis juga meluas ke ranah teknologi informasi melalui penerapan RME, yang memungkinkan pengolahan data digital secara efisien dan terintegrasi dalam sistem informasi rumah sakit, meningkatkan kecepatan penyediaan informasi serta mengurangi beban kerja administratif petugas pelayanan kesehatan (Wardani et al., 2022).

c. Keamanan Informasi Rekam Medis Elektronik

Keamanan informasi merupakan upaya sistematis untuk melindungi informasi dari akses, penggunaan, pengungkapan, perubahan, atau perusakan yang tidak sah. Keamanan informasi RME menjadi aspek penting karena rekam medis memuat data pribadi dan

informasi klinis pasien yang bersifat rahasia. Fasilitas pelayanan kesehatan wajib menjamin keamanan, kerahasiaan, keutuhan, dan ketersediaan data rekam medis, baik dalam bentuk manual maupun elektronik. Ketentuan tersebut menunjukkan bahwa keamanan informasi bukan hanya aspek teknis, tetapi merupakan kewajiban hukum yang melekat pada pengelolaan RME (Permenkes RI No. 24, 2022).

Keamanan informasi pada Rekam Medis Elektronik (RME) merupakan aspek penting untuk melindungi data dan informasi kesehatan dari berbagai ancaman yang dapat mengganggu pengelolaannya. Penerapan keamanan informasi didasarkan pada prinsip kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) untuk memastikan informasi tetap terlindungi, akurat, dan dapat digunakan sesuai kebutuhan. Ketiga prinsip tersebut menjadi dasar dalam menjaga keamanan data sehingga informasi kesehatan hanya dapat diakses oleh pihak yang berwenang, terhindar dari perubahan yang tidak sah, serta tersedia saat diperlukan dalam pelayanan kesehatan (Peraturan BSSN No. 4, 2021).

Keamanan informasi RME yang tidak optimal dapat menimbulkan berbagai risiko serius. Risiko tersebut meliputi kebocoran data pribadi pasien, akses tidak sah oleh pihak yang tidak berwenang, kesalahan pengambilan keputusan klinis akibat perubahan data, serta gangguan pelayanan akibat sistem yang tidak tersedia saat

dibutuhkan. Lemahnya pengendalian keamanan pada sistem RME sering disebabkan oleh kurangnya kebijakan keamanan yang jelas, keterbatasan kompetensi sumber daya manusia, serta pengamanan teknologi yang belum memadai. Kondisi ini berpotensi menimbulkan dampak hukum, menurunkan kepercayaan pasien, dan mengganggu keberlangsungan pelayanan kesehatan (Budiman et al., 2025).

3. Sistem Manajemen Keamanan Informasi (SMKI)

Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management System* (ISMS) merupakan kerangka kerja manajerial yang dirancang untuk melindungi aset informasi organisasi, termasuk data yang dikelola oleh sistem informasi rumah sakit. SMKI mencakup penetapan kebijakan, struktur organisasi, prosedur, serta pengendalian risiko untuk menjamin kerahasiaan, integritas, dan ketersediaan informasi yang kritikal dalam pelayanan kesehatan. Perancangan SMKI yang efektif harus mengacu pada standar nasional maupun standar internasional (Peaturan BSSN No.8, 2020).

Tujuan utama penerapan SMKI dalam pengelolaan RME adalah untuk memastikan bahwa data medis pasien hanya dapat diakses oleh pihak yang berwenang, tetap akurat selama siklus pelayanan, dan tersedia saat dibutuhkan untuk kebutuhan klinis dan administratif. Dalam kerangka SMKI terdapat regulasi internasional terkait perlindungan data kesehatan dan privasi yang relevan untuk keamanan informasi di sistem informasi rumah sakit, antara lain:

a. HIPAA (*Health Insurance Portability and Accountability Act*)

HIPAA adalah regulasi di Amerika Serikat yang fokus pada perlindungan informasi kesehatan pasien (*Protected Health Information*/PHI) dalam sistem elektronik seperti RME. Regulasi ini mewajibkan fasilitas layanan kesehatan menerapkan pengamanan administratif, teknis, dan fisik terhadap data pasien untuk menjamin kerahasiaan, integritas, dan ketersediaan data tersebut. HIPAA juga menekankan perlunya kontrol akses yang ketat dan kewajiban penerapan kebijakan keamanan data untuk mencegah akses tidak sah dan pelanggaran privasi pasien, sehingga menjadi acuan penting dalam desain SMKI di konteks global (Herisasono, 2024).

b. GDPR (*General Data Protection Regulation*)

General Data Protection Regulation (GDPR) adalah regulasi perlindungan data pribadi yang diterapkan oleh Uni Eropa untuk memberikan perlindungan yang lebih kuat terhadap data pribadi individu. GDPR mengatur prinsip pemrosesan data pribadi, termasuk transparansi, keadilan, legalitas, pembatasan tujuan, minimalisasi data, akurasi, pembatasan penyimpanan, serta integritas dan kerahasiaan data. GDPR juga memberikan hak kepada individu untuk mengakses, memperbaiki, dan mengendalikan penggunaan data pribadinya oleh organisasi. GDPR bertujuan untuk meningkatkan perlindungan privasi serta memastikan keamanan data pribadi selama proses pengumpulan, penggunaan, penyimpanan, dan pengolahan data (Microsoft, 2024).

c. ISO/IEC 27001:2022

ISO/IEC 27001:2022 merupakan standar internasional yang digunakan sebagai acuan dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI). Standar ini menetapkan persyaratan bagi organisasi dalam membangun, menerapkan, memelihara, dan meningkatkan sistem keamanan informasi secara berkelanjutan untuk menjaga kerahasiaan, keutuhan, dan ketersediaan informasi. Seiring dengan terbitnya ISO/IEC 27001:2022, BSSN juga mengalami penyesuaian untuk mengakomodasi perubahan struktur kontrol keamanan yang sebelumnya mengacu pada ISO/IEC 27001:2013 menjadi mengacu pada ISO/IEC 27001:2022 (Peraturan BSSN No.4, 2021).

Penerapan ISO/IEC 27001:2022 bertujuan untuk memberikan kerangka kerja yang memungkinkan organisasi mengidentifikasi aset informasi, mengenali ancaman dan kerentanan, serta menerapkan pengendalian yang sesuai untuk meminimalkan risiko. Selain melindungi informasi dari berbagai ancaman, penerapan standar ini juga mendukung kepatuhan terhadap peraturan yang berlaku, meningkatkan kepercayaan pemangku kepentingan, serta memperkuat tata kelola keamanan informasi organisasi. Oleh karena itu, ISO/IEC 27001:2022 menjadi salah satu standar yang digunakan dalam pengukuran tingkat kematangan keamanan informasi melalui Indeks KAMI (BSSN, 2025).

ISO/IEC 27001:2022 terdiri atas klausul 4 sampai dengan klausul 10 yang menjadi persyaratan utama dalam penerapan SMKI. Klausul tersebut meliputi konteks organisasi, kepemimpinan, perencanaan, dukungan, operasional, evaluasi kinerja, dan peningkatan berkelanjutan yang membentuk suatu siklus pengelolaan keamanan informasi secara terintegrasi. Standar ini juga memiliki *Annex A* yang berisi kontrol keamanan informasi yang digunakan sebagai dasar dalam pengelolaan risiko keamanan informasi. ISO/IEC 27001:2022 terdiri atas 93 kontrol yang dikelompokkan ke dalam empat kategori, yaitu *organizational controls, people controls, physical controls, dan technological controls* (BSSN,2025).

4. Indeks Keamanan Informasi (KAMI)

Indeks Keamanan Informasi atau Indeks KAMI v5.0 merupakan instrumen penilaian yang dikembangkan oleh Badan Siber dan Sandi Negara (BSSN) untuk mengukur tingkat kesiapan penerapan keamanan informasi pada suatu organisasi. Indeks KAMI v5.0 disusun sebagai alat bantu evaluasi mandiri (*self-assessment*) yang mengacu pada kerangka Sistem SMKI berstandar ISO/IEC 27001. Penggunaan Indeks KAMI v5.0 sebagai instrumen nasional dalam menilai kesiapan pengamanan sistem elektronik pada instansi pemerintah maupun sektor strategis lainnya, termasuk fasilitas pelayanan kesehatan (Peraturan BSSN No. 9, 2021).

Tujuan utama pengembangan Indeks KAMI v5.0 adalah untuk membantu organisasi memahami posisi dan tingkat kesiapan keamanan

informasi yang telah diterapkan sebelum melaksanakan sertifikasi atau audit keamanan informasi secara formal. Indeks KAMI v5.0 digunakan untuk mengidentifikasi kesenjangan antara kondisi aktual pengamanan informasi dengan persyaratan standar ISO/IEC 27001, sehingga organisasi dapat mengetahui area yang masih perlu diperbaiki atau ditingkatkan. Pedoman BSSN menegaskan bahwa hasil Indeks KAMI v5.0 bersifat diagnostik dan rekomendatif, bukan sebagai alat penilaian kepatuhan atau audit sertifikasi (Peraturan BSSN No. 9, 2021).

Instrumen Indeks KAMI mengalami pengembangan dari versi 4.2 ke versi 5.0 seiring dengan pembaruan standar ISO/IEC 27001. Indeks KAMI versi 4.2 disusun dengan mengacu pada ISO/IEC 27001:2013 dan menilai lima area utama keamanan informasi. Indeks KAMI v5.0 disesuaikan dengan ISO/IEC 27001:2022 dan menambahkan satu area baru, yaitu pelindungan data pribadi, sehingga total area penilaian menjadi enam. Penambahan area tersebut dilakukan untuk menyesuaikan Instrumen dengan perkembangan regulasi dan kebutuhan perlindungan data pribadi yang semakin kompleks, khususnya pada sistem elektronik yang mengelola data sensitif seperti RME (Ramadhan et al., 2025).

Penilaian Indeks KAMI v5.0 dilakukan dengan cakupan keseluruhan persyaratan pengamanan yang tercantum dalam standar SNI ISO/IEC 27001. Pada proses penilaian Indeks KAMI v5.0 terdapat kategori sistem elektronik sebagai gambaran status kesiapan keamanan informasi elektronik. Kategori sistem elektronik ini digunakan sebagai gambaran awal

status kesiapan keamanan informasi elektronik organisasi dan menjadi dasar dalam interpretasi hasil penilaian. Suplemen berfungsi untuk menilai mekanisme pengamanan terkait keterlibatan pihak ketiga eksternal dalam operasional penyelenggaraan layanan informasi. Suplemen ini digunakan untuk memastikan bahwa pengelolaan risiko keamanan informasi tidak hanya mencakup proses internal organisasi, tetapi juga mempertimbangkan risiko yang timbul dari kerja sama dengan pihak eksternal. Setelah tahap awal tersebut, penilaian dilanjutkan pada enam area sebagai tingkat kesiapan keamanan informasi. Berikut enam area penilaian Indeks KAMI v5.0 yaitu:

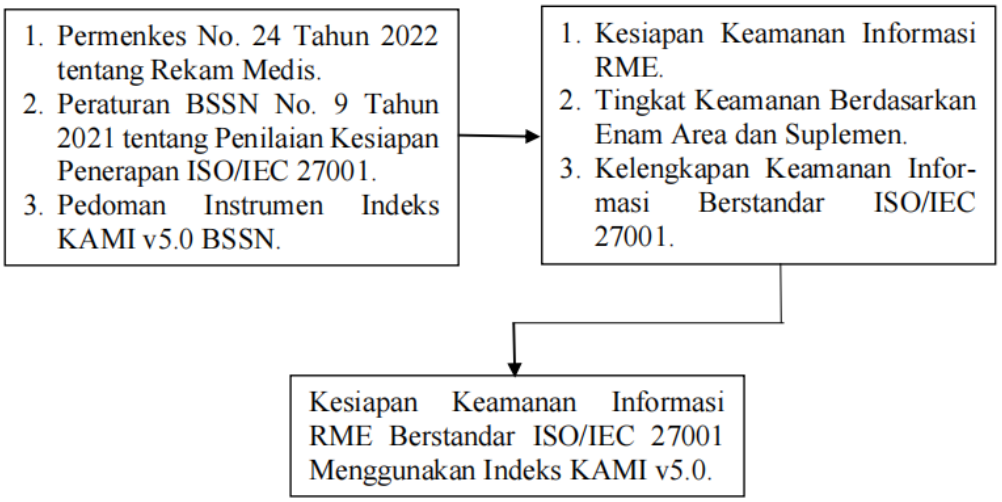
a. Area tata kelola.
b. Area pengelolaan risiko.
c. Area kerangka kerja.
d. Area pengelolaan aset.
e. Area teknologi.
f. Area pelindungan data pribadi.

Penilaian diisi oleh responden kunci yang memiliki kewenangan dan pemahaman menyeluruh terhadap penerapan keamanan informasi di organisasi, seperti penanggung jawab teknologi informasi, pengelola Sistem Manajemen Keamanan Informasi, atau pihak yang ditunjuk secara resmi oleh pimpinan instansi. Penggunaan satu responden kunci dalam penilaian Indeks KAMI v5.0 dinilai memadai secara metodologis, karena instrumen ini tidak mengukur persepsi individu, melainkan mengevaluasi kondisi

organisasi berdasarkan dokumen kebijakan, prosedur, dan bukti penerapan yang dapat dipertanggungjawabkan (BSSN, 2025).

Indeks KAMI v5.0 dirancang sebagai alat ukur kesiapan, bukan sebagai audit keamanan informasi. Hasil penilaian menunjukkan tingkat kematangan dan kesiapan organisasi dalam menerapkan SMKI, namun tidak menghasilkan pernyataan kepatuhan atau sertifikasi. Instrumen ini berfungsi untuk mengetahui kesiapan awal organisasi sebelum melangkah ke tahap implementasi penuh atau sertifikasi ISO/IEC 27001 (BSSN, 2025).

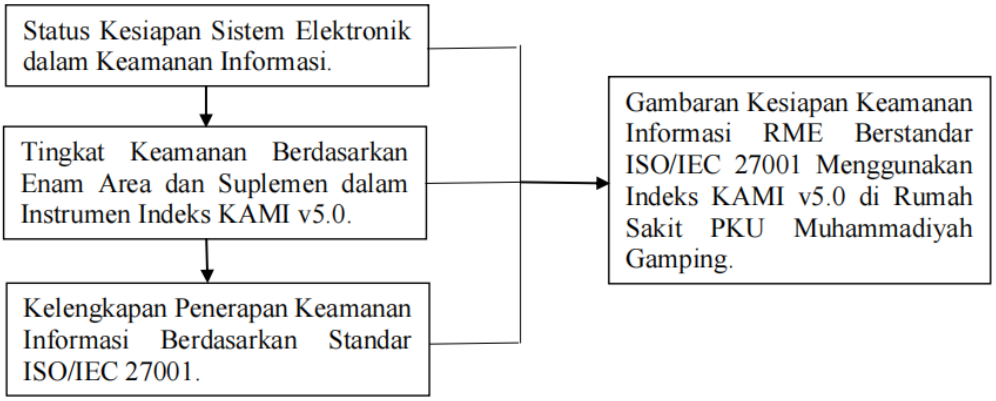
B. Kerangka Teori



Gambar 1. Kerangka Teori.

Sumber: Adaptasi Regulasi Terkait Kesiapan Keamanan Informasi Rekam Medis Elektronik Berstandar ISO/IEC 27001 Menggunakan Indeks KAMI v5.0.

C. Kerangka Konsep



Gambar 2. Kerangka Konsep.

D. Pertanyaan Penelitian

1. Bagaimana status kesiapan keamanan informasi rekam medis elektronik pada kategori sistem elektronik menggunakan Indeks KAMI v5.0 di Rumah Sakit PKU Muhammadiyah Gamping?
2. Bagaimana tingkat kesiapan keamanan informasi RME melalui enam area pengelolaan informasi (tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, teknologi dan keamanan informasi serta perlindungan data pribadi) serta suplemen berdasarkan Instrumen Indeks KAMI v5.0 di Rumah Sakit PKU Muhammadiyah Gamping?
3. Bagaimana kelengkapan penerapan standar ISO/IEC 27001:2022 sesuai Instrumen Indeks KAMI v5.0 di Rumah Sakit PKU Muhammadiyah Gamping?