# BAB I
# PENDAHULUAN

## A. Latar Belakang

Perkembangan teknologi di era modern memberikan pengaruh yang signifikan terhadap hampir seluruh aspek kehidupan manusia. Salah satu konsep yang muncul dari kemajuan ini adalah *Society 5.0*, yang menekankan pemanfaatan teknologi seperti kecerdasan buatan dan analisis *big data* untuk meningkatkan kesejahteraan masyarakat. Konsep ini mendorong transformasi besar dalam layanan publik, termasuk di bidang kesehatan (Rosmayati & Maulana, 2024). Sejalan dengan itu, sistem kesehatan kini mengalami transformasi digital sebagai upaya meningkatkan mutu layanan dan efisiensi (Tenda et al., 2024). Kemajuan ini tidak hanya menjadi simbol modernisasi, tetapi juga landasan bagi inovasi dalam sektor kesehatan seperti rekam medis elektronik dan *telemedicine* yang membuat layanan lebih cepat dan mudah diakses.

Meskipun transformasi digital membawa dampak positif terhadap efisiensi dan mutu pelayanan kesehatan, kemajuan ini juga diikuti oleh meningkatnya risiko terhadap ketahanan dan keamanan sistem. Natakusumah et al., (2022) menjelaskan bahwa penerapan teknologi dalam sektor kesehatan memang berkontribusi pada peningkatan kualitas hidup masyarakat, tetapi juga menimbulkan tantangan baru dalam hal kesiapan infrastruktur digital, integrasi data, serta perlindungan informasi pasien. Wasserman & Wasserman (2022) rumah sakit masih menghadapi berbagai celah keamanan, seperti lemahnya manajemen keamanan data, rendahnya kesadaran tenaga kesehatan mengenai privasi data, serta ketidaksiapan sistem dalam menghadapi serangan siber, kondisi tersebut dapat meningkatkan kerentanan terhadap insiden kebocoran data.

Kebocoran masih menjadi masalah serius yang mengancam privasi masyarakat tidak hanya di Indonesia tapi juga dunia. Dalam beberapa tahun terakhir, isu kebocoran data di sektor kesehatan maupun layanan publik semakin sering terjadi dan skalanya pun makin besar, sehingga mendorong

perlunya penguatan keamanan informasi di berbagai institusi. Secara global, Bright Defense melaporkan bahwa pada 2024 terdapat sekitar 275 juta data kesehatan yang bocor dari berbagai fasilitas layanan, terutama akibat serangan peretas, *ransomware*, serta celah pada pengamanan sistem. Temuan ini menunjukkan bahwa ekosistem kesehatan digital di seluruh dunia masih berada dalam kondisi yang sangat rentan.

Situasi serupa terlihat di Indonesia. Dugaan kebocoran data BPJS Kesehatan yang disebut mencapai 279 juta penduduk menimbulkan kehebohan karena informasi sensitif seperti NIK, alamat, hingga nomor kepesertaan diduga tersebar di forum daring. Besarnya skala dugaan kebocoran ini yang hampir menyamai jumlah total penduduk Indonesia mendorong pemerintah melakukan penelusuran lebih lanjut, mengingat dampaknya dapat memengaruhi kepercayaan masyarakat terhadap layanan publik.

Di level daerah, kekhawatiran masyarakat kembali meningkat setelah muncul klaim bahwa data pribadi sekitar 4,6 juta warga Jawa Barat bocor dan dijual di dark web. Meskipun Pemprov Jabar memastikan bahwa data resmi mereka tidak ikut bocor, pihak Diskominfo Jabar mengakui bahwa upaya peretasan memang pernah terjadi, namun hingga kini mereka masih mampu menjaga keamanan data yang dikelola. Hal ini menunjukkan bahwa serangan siber bukan lagi ancaman sesekali, tetapi situasi yang terus berlangsung dan membutuhkan kewaspadaan yang konsisten. Kondisi tersebut menggambarkan masih lemahnya perlindungan sistem data publik di Indonesia, termasuk di sektor kesehatan. Oleh karena itu, isu keamanan data penting untuk menjadi perhatian utama bagi transformasi digital dalam layanan kesehatan, terutama karena semakin banyaknya ancaman yang menargetkan sistem informasi kesehatan.

Salah satu sistem yang paling rentan terdampak oleh meningkatnya ancaman keamanan data adalah Rekam Medis Elektronik (RME). Sistem ini berfungsi sebagai pusat penyimpanan informasi pasien, mencakup identitas, riwayat penyakit, hasil pemeriksaan, dan tindakan medis yang

dilakukan. Karena sifatnya yang terintegrasi dengan berbagai unit pelayanan, gangguan atau kebocoran pada sistem RME dapat berdampak luas terhadap operasional rumah sakit dan kepercayaan masyarakat terhadap layanan kesehatan digital (Wijayanti et al., 2024). Pribadi et al., (2025) menyebutkan bahwa kelemahan pada satu bagian sistem informasi dapat membuka peluang akses ilegal terhadap keseluruhan data rumah sakit. Oleh karena itu, keamanan data RME menjadi hal yang penting dalam menjaga berjalannya sistem pelayanan kesehatan digital.

Keamanan data RME menjadi aspek yang penting dalam mendukung keberlanjutan sistem pelayanan kesehatan digital. Perlindungan terhadap data medis tidak hanya mencakup penerapan aspek teknis seperti enkripsi dan *firewall*, tetapi juga kebijakan, prosedur, serta kesadaran pengguna dalam menjaga kerahasiaan informasi, dan penting untuk dilakukannya penguatan regulasi (WHO, 2021). Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (2022) tentang Perlindungan Data Pribadi menegaskan bahwa data medis termasuk kategori data sensitif yang wajib dilindungi secara ketat. Soraya et al. (2025) menyebutkan bahwa penerapan sistem keamanan yang baik pada RME tidak hanya menjaga integritas data, tetapi juga meningkatkan kepercayaan publik terhadap layanan kesehatan digital serta memperkuat kualitas pengambilan keputusan klinis.

Salah satu penelitian yang sudah dilakukan sebelumnya telah mengkaji aspek keamanan Rekam Medis Elektronik (RME) di berbagai fasilitas kesehatan. Wardani et al., (2024) menyebutkan enam komponen utama keamanan RME, yakni privasi, integritas, autentikasi, ketersediaan, kontrol akses, dan *non-repudiation*.

Meskipun penelitian sebelumnya telah menganalisis berbagai kelemahan dalam sistem keamanan RME, seperti penggunaan kata sandi *default*, kurangnya fitur *logout* otomatis, serta lemahnya pengawasan terhadap ruang server, penelitian tersebut umumnya masih terbatas pada penilaian aspek keamanan tertentu saja dan belum menggunakan

pendekatan manajemen risiko yang sistematis untuk mengevaluasi seluruh risiko secara menyeluruh. Kondisi ini menunjukkan adanya kesenjangan penelitian, yaitu belum adanya analisis mendalam terhadap aset informasi, ancaman, kerentanan, serta prioritas perlindungan data pasien.

Dalam kondisi ini, penerapan metode *OCTAVE Allegro* menjadi sangat penting. Metode ini mampu mengidentifikasi aset informasi yang paling kritis, menilai risiko yang mungkin terjadi, serta menetapkan prioritas pengendalian risiko berdasarkan konteks rumah sakit secara menyeluruh. Keunggulan *OCTAVE Allegro* terletak pada kemampuannya mengevaluasi risiko tidak hanya dari aspek teknis, tetapi juga dari kebijakan dan perilaku pengguna, sehingga hasilnya lebih komprehensif dan aplikatif (Caralli et al., 2007). Penelitian menunjukkan bahwa metode ini dapat mendeteksi risiko tinggi, seperti gangguan server dan kebocoran data pasien, serta menghasilkan rekomendasi pengendalian yang realistis sesuai kondisi fasilitas. Dengan demikian, penggunaan *OCTAVE Allegro* sangat penting untuk merancang strategi perlindungan data yang efektif, efisien, dan berkelanjutan, sekaligus meningkatkan kepercayaan masyarakat terhadap layanan kesehatan digital (Diahapsari & Riadi, 2022).

Hasil studi pendahuluan yang dilakukan di RSUD dr. Soekardjo Tasikmalaya melalui wawancara dengan petugas SIMRS, IT, dan Rekam Medis menunjukkan bahwa rumah sakit menggunakan SIMRS *SIMGos* dari Kementerian Kesehatan yang bersifat *open source* dan dikelola secara mandiri. Akses sistem diberikan kepada pengguna berwenang seperti PMIK, dokter, perawat, dan admin unit dengan penggunaan akun dan kata sandi sesuai hak akses masing-masing. Server sistem ditempatkan dan dikelola di lingkungan rumah sakit, namun pengelolaan infrastruktur dan dukungan teknis masih terbatas. Saat ini pencadangan data dilakukan satu kali setiap hari, praktik ini masih dapat diterima pada fasilitas pelayanan kesehatan yang sedang menyesuaikan kapasitas teknologi dan sumber daya. Namun, dengan karakteristik data SIMRS yang bersifat dinamis dan terus berubah selama pelayanan berlangsung, perlu dilakukan evaluasi apakah frekuensi

pencadangan harian tersebut sudah mencukupi untuk mengurangi risiko kehilangan data atau diperlukan mekanisme pencadangan yang lebih sering atau otomatis sesuai standar praktik terbaik keamanan informasi.

Mekanisme keamanan sistem saat ini dilakukan melalui penggunaan *username* dan *password* serta pembatasan akses. Berdasarkan pernyataan petugas, potensi risiko terhadap keamanan data pada SIMRS di RSUD dr. Soekardjo Tasikmalaya masih dapat terjadi, baik dari aspek teknis maupun non-teknis. Kondisi tersebut dinilai semakin berpotensi terjadi karena belum adanya pelatihan khusus mengenai keamanan data pasien bagi pengguna sistem secara optimal, padahal petugas menilai pelatihan tersebut perlu dilakukan agar pemahaman terkait keamanan informasi lebih merata, terutama seiring dengan bertambahnya jumlah pengguna sistem dan meningkatnya potensi risiko kebocoran data.

Kondisi tersebut menunjukkan bahwa meskipun sistem sudah berjalan dan memiliki mekanisme pengamanan dasar, masih terdapat potensi risiko dari aspek teknis maupun non-teknis. Hal ini memperkuat perlunya dilakukan analisis risiko keamanan informasi secara menyeluruh untuk mengidentifikasi aset penting, ancaman, dan kerentanan pada sistem RME menggunakan metode *OCTAVE Allegro*, sehingga hasilnya dapat memberikan rekomendasi pengendalian yang tepat dan sesuai dengan kondisi nyata rumah sakit. Dengan demikian, penelitian ini diharapkan mampu menghasilkan analisis risiko yang mendalam guna memperkuat perlindungan data pasien serta meningkatkan kepercayaan masyarakat terhadap layanan kesehatan digital.

## B. Rumusan Masalah

Rumusan masalah penelitian adalah ” Bagaimana Penerapan dan Penilaian Terhadap Penggunaan Keamanan Sistem Rekam Medis Elektronik di RSUD dr. Soekardjo Tasikmalaya berdasarkan metode *OCTAVE Allegro*?”

## C. Tujuan Penelitian

1. Tujuan Umum

   Tujuan dari penelitian ini adalah untuk mengetahui penggunaan sistem keamanan sistem Rekam Medis Elektronik (RME) di RSUD dr. Soekardjo Tasikmalaya berdasarkan metode *OCTAVE Allegro*, guna mengetahui tingkat kesiapan rumah sakit dalam melindungi data dan informasi pasien serta memberikan rekomendasi dalam memperkuat upaya perlindungan data dan informasi pasien.

2. Tujuan Khusus
   a. Mengidentifikasi aset informasi kritis pada Sistem RME.
   b. Mengidentifikasi potensi ancaman serta kerentanan yang dapat mempengaruhi sistem RME di rumah sakit.
   c. Melakukan analisis tingkat risiko keamanan informasi pada Sistem RME.
   d. Merumuskan rekomendasi kontrol keamanan yang sesuai berdasarkan hasil analisis risiko menggunakan *OCTAVE Allegro*.

## D. Manfaat Penelitian

1. Manfaat Praktis
   a. Memberi gambaran umum mengenai tingkat keamanan sistem Rekam Medis Elektronik (RME) di RSUD dr. Soekardjo Tasikmalaya berdasarkan hasil analisis menggunakan metode *OCTAVE Allegro*.
   b. Membantu manajemen rumah sakit dalam merencanakan langkah-langkah strategis untuk memperkuat sistem keamanan data pasien dan meningkatkan layanan informasi kesehatan digital.
   c. Menjadi acuan bagi fasilitas pelayanan kesehatan lain yang ingin melakukan penilaian atau peningkatan keamanan sistem Rekam Medis Elektronik (RME).

2. Manfaat Teoritis
   a. Memberikan kontribusi terhadap pengembangan kajian ilmiah di bidang manajemen risiko keamanan informasi kesehatan, khususnya dalam penerapan metode *OCTAVE Allegro* pada sistem Rekam Medis Elektronik (RME).
   b. Memperkuat referensi akademik terkait metode *OCTAVE Allegro* sebagai alat analisis risiko keamanan informasi yang menyeluruh di lingkungan fasilitas pelayanan kesehatan.

## E. Keaslian Penelitian

*Tabel 1. 1.Keaslian Penelitian*

| No | Nama Peneliti | Judul | Persamaan | Perbedaan |
|---|---|---|---|---|
| 1. | Wardani E., Putra, D. H., Sonia, D., & Yulia, N. (2024) | Keamanan Sistem Informasi Rekam Medis Elektronik di Rumah Sakit Islam Jakarta Sukapura | Memiliki metode yang sama yaitu *OCTAVE Allegro* | Pada Wardani, E., Putra, D. H., Sonia, D., & Yulia, N. (2024) konteks penelitian di fokuskan pada kelemahan fitur logout otomatis dan penggunaan password default, sedangkan penelitian penulis fokus pada penilaian risiko menyeluruh dan prioritas mitigasi pada RME di RSUD |

| | | | | |
|---|---|---|---|---|
| 2. | Hapsari, R. & Subiyantoro, D (2025) | *Gambaran Sistem Keamanan Rekam Medis Elektronik di RS AL dr. Mintohardjo Jakarta menggunakan OCTAVE Allegro* | Memiliki metode yang sama yaitu *OCTAVE Allegro* sebagai bagian dari proses penilaian risiko informasi | Pada Penelitian Hapsari, R. & Subiyantoro, D. (2025) konteks penelitian ini di fokuskan pada kelemahan kontrol akses dan pengawasan ruang server, sedangkan penelitian penulis fokus pada analisis tingkat risiko per aset dan rekomendasi pengendalian |
| 3. | Arinda Diahapsari & Imam Riadi, (2022) | *Analysis Risk Assessment on Hospital Management Information System using OCTAVE Allegro Framework* | Memiliki metode yang sama yaitu menggunakan *OCTAVE Allegro* dalam penilaian risiko sistem informasi berbasis aset | Pada penelitian Arinda Diahapsari & Imam Riadi (2022) objek penelitian ini melakukan evaluasi pada SIMRS secara keseluruhan, sedangkan penelitian penulis spesifik pada keamanan sistem |

| | |
|---|---|
| | Rekam Medis Elektronik (RME) di RSUD dr. Soekardjo |