BAB I
PENDAHULUAN

A. Latar Belakang

Pemanfaatan teknologi informasi dalam bentuk Sistem Informasi Manajemen Puskesmas (SIMPUS) telah menjadi standar dalam upaya meningkatkan mutu layanan dan efisiensi manajemen di Puskesmas. SIMPUS berfungsi menyediakan informasi yang akurat untuk mendukung proses pengambilan keputusan dan pencapaian sasaran kegiatan Puskesmas secara efektif (Gavinov & Lestari, 2022). Sebagai fasilitas layanan kesehatan tingkat pertama, Puskesmas memerlukan pengelolaan data pasien yang tertata dengan baik guna menjamin kelancaran evaluasi kinerja, penyusunan kebijakan, dan peningkatan layanan kesehatan masyarakat.

Dalam konteks digitalisasi layanan, pengelolaan data yang baik harus didukung dengan sistem yang mampu menjamin keamanan informasi. Data pasien yang bersifat sensitif harus dilindungi dari akses pihak yang tidak berwenang. Oleh karena itu, aspek keamanan informasi menjadi bagian integral dari sistem informasi manajemen yang diterapkan. Keamanan sistem informasi bertujuan untuk menjaga tiga aspek penting, yaitu kerahasiaan, integritas, dan keaslian data (Wiranata et al., 2023). Tanpa adanya perlindungan yang memadai, keberadaan sistem informasi justru dapat menjadi celah risiko yang membahayakan organisasi.

Berdasarkan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Pasal 1 (2016) Pemerintah Indonesia, data pribadi adalah informasi spesifik tentang individu yang dijaga, dipelihara, dan dilindungi keakuratannya, dengan langkah-langkah yang diambil untuk melindungi kerahasiaannya. Jika data tersebut disalahgunakan dan jatuh ke tangan orang yang tidak berwenang, hal tersebut dapat mengakibatkan kerugian yang signifikan bagi pemilik informasi yang sah. Kebocoran atau penyalahgunaan data pasien bukan hanya dapat merugikan pihak individu yang datanya dicuri, tetapi juga dapat merusak kredibilitas institusi

pelayanan kesehatan seperti Puskesmas (Kusuma & Rahmani, 2022). Data pasien yang bocor ke pihak yang tidak berwenang dapat digunakan untuk tujuan komersial, manipulasi, atau bahkan tindakan kriminal lainnya. Oleh karena itu, penting untuk memastikan bahwa sistem informasi yang digunakan telah memenuhi standar keamanan yang baik. Penilaian faktor keamanan ini dapat dilakukan dengan menggunakan metode Kerahasiaan, Integritas, dan Ketersediaan, yang biasa disebut sebagai kerangka kerja. Pendekatan ini bertujuan untuk memastikan bahwa data hanya dapat diakses oleh pihak yang berwenang, tidak diubah tanpa izin, dan selalu tersedia ketika dibutuhkan (Firmansyah et al., 2025).

Berdasarkan Peraturan Mentri Kesehatan Nomor 24 tahun 2022, menjelaskan bahwasannya rekam medis elektronik harus memenuhi prinsip keamanan data dan informasi. Kerahasiaan sebagaimana dimaksud pada ayat (1) merupakan jaminan keamanan data dan informasi dari gangguan pihak internal maupun eksternal yang tidak memiliki hak akses, sehingga data dan informasi yang ada dalam Rekam Medis Elektronik terlindungi penggunaan dan penyebarannya. Integritas sebagaimana dimaksud pada ayat (1) merupakan jaminan terhadap keakuratan data dan informasi yang ada dalam Rekam Medis Elektronik, dan perubahan terhadap data hanya boleh dilakukan oleh orang yang diberi hak akses untuk mengubah. Ketersediaan sebagaimana dimaksud pada ayat (1) merupakan jaminan data dan informasi yang ada dalam Rekam Medis Elektronik dapat diakses dan digunakan oleh orang yang telah memiliki hak akses yang ditetapkan oleh pimpinan Fasilitas Pelayanan Kesehatan.

Evaluasi keamanan data berbasis *Confidentiality* (Kerahasiaan), *Integrity* (Keutuhan), *Availability* (Ketersediaan) di lingkungan Puskesmas menjadi semakin relevan mengingat Puskesmas merupakan fasilitas pelayanan kesehatan primer yang bersentuhan langsung dengan masyarakat luas. Dengan jumlah pasien yang banyak dan proses digitalisasi yang masih berkembang, risiko kesalahan teknis maupun administratif dalam pengelolaan data menjadi tinggi (Kambey et al., 2018). Oleh karena itu,

penelitian ini tidak hanya akan menilai aspek teknis dari sistem yang digunakan, tetapi juga akan mempertimbangkan faktor manusia, prosedur operasional, dan kebijakan internal yang berkaitan dengan pengamanan data. Harapannya adalah bahwa temuan dari penilaian ini akan menawarkan gambaran luas tentang status perlindungan data pasien dan berfungsi sebagai landasan untuk meningkatkan strategi dan kerangka kerja keamanan informasi di Pusat Kesehatan di masa mendatang.

Puskesmas Sedayu 2 merupakan puskesmas yang berada di Daerah Istimewa Yogyakarta. Puskesmas Sedayu 2 sudah mengimplementesikan sistem Rekam Medis Elektronik (RME) sejak Tahun 2019 dengan menggunakan versi 2 kemudian pada tahun 2024 berubah menjadi versi 3. Sebanyak 39 petugas puskesmas yang menggunakan RME sejak dari tahun 2019. Puskesmas sedayu 2 hanya melakukan monitoring dan evaluasi bulanan ketika simpus error atau penambahan item, sehingga evaluasi simpus di puskesmas sedayu 2 sangat jarang dilakukan. Evaluasi yang dilakukan dari Dinas Kesehatan kepada Puskesmas Sedayu 2 juga tidak rutin dilakukan dan hanya ketika menerima undangan saja.

Berdasarkan setudi pendahuluan di puskesmas sedayu 2, pada sistem informasi puskesmas sudah berjalan dengan baik. Pada puskesmas sedayu 2 juga untuk pelayanan sudah menggunakan rekam medis elektronik semua. Meskipun puskesmas telah menggunakan sistem informasi puskesmas dengan baik, tetapi masih terdapat resiko seperti beberapa petugas masih menyimpan *username* dan *password* secara otomatis pada bagian *login* pengguna, hal ini berpotensi tinggi terhadap keamanan data, karena dapat membuka celah bagi pihak yang tidak berwenang untuk mengakses data rekam medis pasien. Selain itu juga terdapat masalah dibagian sistem informasi manajemen puskesmas (SIMPUS) telah dilengkapi dengan fitur *auto logout* sebagai salah satu upaya pengamanan akses pengguna. Fitur ini dirancang untuk secara otomatis mengeluarkan pengguna dari sistem apabila tidak ada aktivitas dalam jangka waktu tertentu. Durasi auto *logout* pada SIMPUS di Puskesmas Sedayu II masih terbilang sangat lama, bahkan bisa mencapai beberapa jam sebelum sistem melakukan *logout* otomatis. Kondisi ini berpotensi menimbulkan risiko serius terhadap keamanan data rekam medis pasien

seperti kebocoran data. Berdasarkan latar belakang diatas maka penulis tertarik untuk melakukan penelitian tentang judul "Evaluasi Keamanan SIMPUS Berdasarkan Aspek *Confidentiality, Integrity, Availability* di Puskesmas Sedayu ll".

B. Rumusan Masalah

Bagaimana keamanan data pasien pada sistem informasi manajemen puskesmas berdasarkan aspek confidentiality, integrity, dan availability dipuskesmas Sedayu II.

C. Tujuan Penelitian

1. Tujuan Umum

   Menillai keamanan data pasien dan mengetahui bagaimana keamanan SIMPUS di puskesmas Sedayu II.

2. Tujuan Khusus
   a. Menganalisis keamanan data pasien pada SIMPUS di puskesmas Sedayu II berdasarkan aspek *confidentiality*.
   b. Menganalisis keamanan data pasien pada SIMPUS di puskesmas Sedayu II berdasarkan aspek *integrity*.
   c. Menganalisis keamanan data pasien pada SIMPUS di puskesmas Sedayu II berdasarkan aspek *availability*.

D. Manfaat Penelitian

1. Manfaat bagi puskesmas

   Manfaat penelitian ini bagi Puskesmas diharapkan dapat menjadi salah satu bahan masukan terkait keamanan SIMPUS sehingga dapat dijadikan pedoman dalam perbaikan sistem informasi manajemen puskesmas.

2. Manfaat penelitian

   Menambah wawasan dan pengetahuan tentang keamanan data pasien pada sistem informasi manajemen puskesmas.

E. Keaslian Penelitian

1.1 Keaslian Penelitian

No	Nama Peneliti	Tahun	Judul Penelitian	Jenis Penelitian	Teknik Sampling	Hasil Penelitian	Persamaan	Perbedaan
1	Esti Setyaningrum, agustinus	2025	Analisis Keamanan Data Pasien Dalam Rekam Medis Elektronik berdasarkan CIA di RSUD X Jawa Tengah	Kualitatif	teknik pengumpulan data, termasuk observasi langsung, wawancara mendalam,	Meningkatkan efisiensi pelayanan kesehatan dengan mempermudah koordinasi antar penyedia layanan dan memastikan informasi pasien tetap terorganisir dengan baik dan mengetahui bagaimana hasil Analisis Keamanan Data Pasien dalam Rekam Medis Elektronik	Dalam penelitian ini dan penulis sama-sama membahasa 3 aspek	Melakukan penelititian keamanan dan privasi rekam medis di rumah sakit sedangkan peneliti di puskesmas
2	Efri Tri Ardianto, Sabran, Lensa Nurjanah	2024	Analisis Aspek Keamanan data Pasien Dalam Implementasi Rekam Medis Elektronik di Rumah Sakit X	Kualitatif	teknik pengumpulan data, termasuk observasi langsung, wawancara mendalam,	Menunjukkan bahwa keamanan dari aspek kerahasiaan yaitu *login* menggunakan *username* & *password* namun belum melakukan penggantian secara berkala serta belum adanya SOP.	Penelitian ini sama-sama menggunakan metode kuali dan sama-sama membahas keamanan data	Dalam penelitian ini menggunakan 5 aspek sedang penulis menggunakan 3 aspek

No	Nama Peneliti	Tahun	Judul Penelitian	Jenis Penelitian	Teknik Sampling	Hasil Penelitian	Persamaan	Perbedaan
3	Soraya, Ervita Nindy	2025	Evaluasi Keamanan dan Privasi Sistem Rekam Medis Elektronik: Studi Kasus di Rumah Sakit Wava Husada	Kualitatif	purposive sampling, menentukan sampel	Memberikan gambaran penting tentang upaya fasilitas kesehatan dalam menjaga privasi pasien dan mematuhi regulasi yang berlaku, serta menjadi referensi bagi peningkatan sistem keamanan informasi di layanan kesehatan lainnya.	Menggunakan metode evaluasi Kualitatif deskriptif	Melakukan penelititian keamanan dan privasi rekam medis di rumah sakit sedangkan peneliti di puskesmas
4	Destri Maya Rani	2025	Evaluasi Keamanan Informasi Sistem Rekam Medis Elektronik di RSI Sultan Agung	Kualitatif	Non probability yaitu menggunakan puposive sampel yang memfokuskan pada informan-informan terpilih,	ditemukan bahwa 53 klausa dari 108 klausa persyaratan yang diminta untuk memenuhi aspek keamanan informasi di RSI Sultan Agung berdasarkan ISO 27001, dengan presentases sebesar 49	Membahas terkait 3 aspek *Confidentiality*, *integrity*, *availability*	Dilakukan di rumah sakit sultan agaung, sedangkan peneliti melakukan di puskesmas

No	Nama Peneliti	Tahun	Judul Penelitian	Jenis Penelitian	Teknik Sampling	Hasil Penelitian	Persamaan	Perbedaan
5	Untung Slamet Suhariyono	2025	Analisis Aspek Keamanan Informasi Data Pasien pada Rekam Medis Elektronik di UPT Puskesmas Karangploso	Kualitatif	purposive sampling, menentukan sampel berdasarkan kriteria atau pertimbangan tertentu	keamanan data pasien dari aspek *confidentiality* sudah sesuai karena sudah ada *username* dan *password* untuk setiap user telah memiliki fitur *log out* otomatis dalam waktu kurang lebih selama satu jam setelah tidak adanya aktivitas yang dilakukan di dalam sistem rekam medis elektronik.	Penelitian dilakukan di puskesmas dengan metode kualitatif	Dialakukan di puskesmas karangploso sedangkan peneliti melakukan di puskesmas sedayu ll