ANALISIS KEAMANAN DATA DAN INFORMASI KESEHATAN PADA SISTEM INFORMASI MANAJEMEN PUSKESMAS (SIMPUS) DI PUSKESMAS WERU

KARYA TULIS ILMIAH

Merupakan Salah Satu Persyaratan Memperoleh Gelar Ahli Madya

Oleh :

ISMEYLIA WIDY NUGRAHENY

NIM : 2352200003

PROGRAM STUDI DIII REKAM MEDIS DAN INFORMASI KESEHATAN

FAKULTAS KESEHATAN MASYARAKAT DAN ILMU KESEHATAN

UNIVERSITAS VETERAN BANGUN NUSANTARA

SUKOHARJO

2026

ABSTRAK

ISMEYLIA WIDY NUGRAHENY. 2352200003. ANALISIS KEAMANAN DATA DAN INFORMASI KESEHATAN PADA SISTEM INFORMASI MANAJEMEN PUSKESMAS (SIMPUS) DI PUSKESMAS WERU. KTI. DIII Rekam Medis dan Informasi Kesehatan. Fakultas Kesehatan Masyarakat dan Ilmu Kesehatan Universitas Veteran Bangun Nusantara. 2026

Keamanan data dan informasi kesehatan merupakan aspek penting dalam melindungi data pasien serta mendukung layanan kesehatan. Penelitian ini bertujuan untuk menganalisis perlindungan data dan informasi pada Sistem Informasi Manajemen Puskesmas (SIMPUS) di Puskesmas Weru berdasarkan pendekatan CIA Triad (*Confidentiality*, *Integrity*, *Availability*). Penelitian ini menggunakan metode deskriptif kualitatif dengan subjek penelitian yaitu petugas yang menggunakan SIMPUS. Data diperoleh melalui wawancara dan pengamatan. Hasil penelitian menunjukkan bahwa aspek *Confidentiality* telah diterapkan melalui penggunaan autentikasi *username* dan *password* serta pembatasan hak akses berdasarkan peran (*Role-Based Access Control*), meskipun terdapat kekurangan dalam kebijakan penggantian *password* dan pelatihan keamanan data. Aspek *Integrity* didukung oleh pengaturan akses, verifikasi data, dan jejak audit untuk memastikan akurasi informasi. Aspek *Availability* dilaksanakan dengan menangani gangguan sistem dan menggunakan formulir manual sebagai solusi saat SIMPUS bermasalah. Kesimpulan penelitian ini menunjukkan data SIMPUS di Puskesmas Weru telah memenuhi aspek kerahasiaan, integritas, dan ketersediaan, namun masih diperlukan peningkatan pada kebijakan pengelolaan *password*, pemerataan pelatihan keamanan data, dan penguatan infrastruktur pendukung sistem.

Kata Kunci: CIA Triad, Keamanan Data, SIMPUS
Kepustakaan: 41 (2017-2026)

Mengetahui
Dekan Fakultas Kesehatan
Masyarakat dan Ilmu Kesehatan

Pembimbing

Prita Devy Igiany, S,Kep., M.P.H
NIDN. 0603049001

Rika Andriani, S.K.M., M.P.H
NIDN. 0613019001

ABSTRACT

ISMEYLIA WIDY NUGRAHENY. 2352200003. ANALISIS KEAMANAN DATA DAN INFORMASI KESEHATAN PADA SISTEM INFORMASI MANAJEMEN PUSKESMAS (SIMPUS) DI PUSKESMAS WERU. KTI. DIII Rekam Medis dan Informasi Kesehatan. Fakultas Kesehatan Masyarakat dan Ilmu Kesehatan Universitas Veteran Bangun Nusantara. 2026

Health data and information security is a crucial aspect in protecting patient *data and supporting healthcare services. This study aims to analyze data and information protection in the Community Health Center Management Information System (SIMPUS) at Weru Community Health Center based on the CIA Triad (Confidentiality, Integrity, and Availability) approach. This study used a qualitative descriptive method, with SIMPUS staff as subjects. Data were obtained through interviews and observations. The results indicate that confidentiality has been implemented through the use of username and password authentication and role-based access control (Role-Based Access Control), although there are shortcomings in password change policies and data security training. Integrity is supported by access management, data verification, and audit trails to ensure information accuracy. Availability is implemented by handling system disruptions and using manual forms as a solution when SIMPUS issues occur. The study concludes that SIMPUS data at Weru Community Health Center meets the confidentiality, integrity, and availability aspects. However, improvements are needed in password management policies, equitable distribution of data security training, and strengthening of the system's supporting infrastructure.*

Keywords: *CIA Triad, Data Security, SIMPUS*
References: *41 (2017-2026)*

BAB I
PENDAHULUAN

A. Latar Belakang

Fasilitas Layanan Kesehatan adalah tempat atau sarana yang digunakan untuk memberikan pelayanan kesehatan kepada individu atau komunitas dengan pendekatan yang bersifat promotif, preventif, kuratif, rehabilitatif, dan paliatif yang dilaksanakan oleh pemerintah pusat, pemerintah daerah, atau masyarakat. Fasilitas pelayanan kesehatan dapat berupa rumah sakit, puskesmas, klinik, apotek, atau tempat praktik mandiri (Permenkes No 19, 2024). Berdasarkan Permenkes No 43 Tahun 2019, Puskesmas sebagai lembaga yang menyelenggarakan pelayanan kesehatan di tingkat pertama yang terlibat langsung dengan masyarakat dan bertanggung jawab atas menyelenggarakan pembangunan kesehatan di wilayah kerjanya. Puskesmas merupakan sebuah organisasi kesehatan yang fungsional dan berperan penting sebagai pusat pengembangan kesehatan masyarakat. Selain itu, puskesmas juga melibatkan masyarakat dalam berbagai kegiatan serta memberikan pelayanan kesehatan yang lengkap dan terpadu (Mamonto, 2022).

CIA Triad adalah dasar penting dalam pengelolaan risiko keamanan informasi yang terdiri dari tiga elemen utama, yaitu kerahasiaan *(confidentiality)*, integritas *(integrity)*, dan ketersediaan *(availability)* (Harahap et al., 2023). CIA Triad merupakan kerangka utama dalam keamanan informasi yang dimanfaatkan oleh organisasi untuk melindungi data dan sistem terhadap ancaman *cyber*. Ketiga pilar tersebut menjamin bahwa data hanya dapat diakses oleh pihak yang berwenang *(Confidentiality)*, tetap akurat dan tidak dimodifikasi tanpa izin *(Integrity)*, serta selalu dapat diakses oleh pengguna yang berhak saat diperlukan *(Availability)*. Ketiga pilar tersebut menjadi dasar bagi perumusan kebijakan ancaman cyber dan saling mengisi dan mendukung organisasi dalam menilai kebutuhan perlindungan mereka terhadap ancaman seperti peretasan, perubahan data secara ilegal, kerusakan sistem, dan gangguan layanan (Lasky, 2024). Setiap elemen dalam CIA Triad memiliki

hubungan
yang saling mendukung dan membentuk satu kesatuan dalam sistem keamanan informasi, oleh karena itu penerapannya harus dilakukan secara menyeluruh dan seimbang. Ketidakseimbangan terhadap salah satu elemen tersebut dapat menyebabkan kerentanan yang signifikan yang berpotensi dimanfaatkan oleh pihak yang tidak berwenang dan berdampak pada terganggunya keamanan serta keandalan sistem informasi. Penerapan prinsip CIA Triad dalam sistem informasi kesehatan sangat penting, karena data pasien tidak hanya dimanfaatkan untuk layanan medis, tetapi juga untuk laporan, evaluasi program, dan pengambilan keputusan. Jika salah satu elemen dari CIA Triad tidak dipenuhi maka risiko kebocoran data, kesalahan informasi medis, serta terhambatnya pelayanan dapat terjadi (Guntur, 2025).

Keamanan informasi merupakan aset penting yang harus dilindungi dan dijaga dengan baik. Secara konseptual, keamanan dipahami sebagai sebuah keadaan atau sifat yang menunjukan perlindungan, yaitu bebas dari ancaman, risiko, serta potensi bahaya. Terwujudnya keamanan memerlukan upaya perlindungan yang terstruktur terhadap berbagai jenis gangguan, baik berasal dari dalam maupun luar, untuk memastikan sistem tetap aman dan terkendali (Betty, 2022). Menurut Peraturan Arsip RI No 15 Tahun 2021 tentang Sistem Informasi Manajemen Keamanan Informasi di Lingkungan Arsip Nasional Indonesia, keamanan informasi berarti memastikan informasi tetap rahasia, utuh, dan bisa diakses saat dibutuhkan. Hubungan antara SIMPUS dengan keamanan sistem pada dasarnya sama dengan kerahasiaan organisasi. Menurut *Health Insurance Portability and Accountability Act* (HIPAA) keamanan informasi harus memenuhi beberapa hal yaitu, 1) Memastikan kerahasiaan, integritas, dan ketersediaan semua informasi kesehatan serta melindungi dalam membuat, menerima, mempertahankan, atau mentransmisikan informasi kesehatan, 2) Melindungi dari ancaman dan bahaya yang diantisipasi secara wajar, 3) Melindungi dari pengguna atau pengungkapan informasi yang diantisipasi secara wajar berdasarkan peraturan privasi, 4) Memastikan kepatuhan tenaga kerja (Subramanian, Sengupta and Xu, 2024).

Masalah keamanan data kini menjadi semakin menghawatirkan karena banyaknya kasus pencurian data. Di Indonesia, pencurian data kesehatan telah menjadi isu yang sering terjadi. Tahun 2020 lalu, diperkirakan sekitar 230.000 data pribadi pasien COVID-19 di Indonesia dicuri dan diperjualbelikan. Peristiwa ini tidak hanya menyebabkan kerugian materi, tetapi juga berdampak pada kesehatan mental korban, yang bisa menghadapi diskriminasi sosial (Rahmadiliyani, 2020). Mengingat pentingnya fasilitas kesehatan dalam menjaga keamanan data pasien saat menerapkan sistem rekam medis elektronik, serta risiko besar bila informasi kesehatan bocor dan digunakan oleh pihak tidak bertanggung jawab, maka berdasarkan observasi dan wawancara dengan petugas, terlihat bahwa pelayanan rekam medis di Puskesmas Sering masih kurang memenuhi standar perlindungan informasi, privasi, dan kerahasiaan data pasien. Sistem keamanan terdiri dari beberapa aspek yaitu, *privacy* atau *confidentiality* yang berkaitan dengan kerahasiaan data pasien, *integrity* berhubungan dengan perubahan data informasi, *autenthication* berhubungan dengan akses informasi, *avaliability* ialah aspek ketersedian yang menekankan pada informasi data pasien jika dibutuhkan oleh pihak terkait, *acces control* adalah aspek yang menekankan cara perizinan seseorang ketika mengakses informasi, *non-repundation* merupakan transaksi informasi atau perubahan informasi (Alia, 2024).

Sistem Informasi Manajemen (SIMPUS) merupakan suatu tatanan yang menyediakan informasi untuk membantu proses pengambilan keputusan dalam melaksanakan manajemen puskesmas dalam mencapai sasaran kegiatanya. Sumber informasi SIMPUS mencangkup pencatatan, pelaporan, survei lapangan, laporan lintas sektor terkait laporan fasilitas pelayanan kesehatan di wilayah kerjanya. SIMPUS memiliki tujuan untuk mewujudkan penyelenggaraan sistem informasi puskesmas yang terintegrasi dan menjamin ketersediaan data dan informasi yang berkualitas, berkesinambungan dan mudah diakses demi meningkatkan kualitas pelayanan (Prabowo, 2024). SIMPUS berfungsi untuk mengatur data mulai dari pendaftaran pasien, registrasi pasien, pemeriksaan pasien hingga pemberian obat kepada pasien.

Data yang dimasukkan disimpan dalam database pasien, kemudian diproses dan dikelompokkan sesuai dengan parameter untuk keperluan pelaporan (Rokim *et al.*, 2024). SIMPUS diharapkan dapat meningkatkan manajemen puskesmas secara lebih berhasil guna dan berdaya guna dengan prosedur pemrosesan data SIMPUS berdasarkan teknologi informasi yang tepat waktu,akurat, lengkap dan efektif untuk mendukung proses pengambilan keputusan manajemen puskesmas (Ivan, 2022).

Berdasarkan hasil penelitian yang dilakukan oleh Saputra, (2017) di Puskesmas Pleret Bantul Yogyakarta peneliti menyatakan bahwa tidak terdapat prosedur tetap (protap) dalam pelaksanaan sistem keamanan data server SIMPUS. Pengamanan hanya dilakukan *password* sebagai satu-satunya bentuk autentikasi. Walaupun pengetahuan petugas terhadap pentingnya keamanan tergolong baik, namun penerapan di lapangan masih kurang optimal dikarenakan petugas seringkali membagikan *password* kepada pihak lain tanpa pengawasan. Selain itu, upaya pengamanan data yang dilakukan Puskesmas hanya sebatas *backup* data rutin setiap bulan oleh koordinasi sistem informasi. Peneliti ini menyimpulkan bahwa aspek tanggung jawab dan pengawasan masih menjadi kelemahan utama dalam menjaga keamanan data server di Puskesmas. Puskesmas Weru Kabupaten Sukoharjo sudah menjalankan Sistem Informasi Manajemen Puskesmas sejak pertengahan tahun 2006, sistem ini mulanya menggunakan *single user* sampai tahun 2011, lalu ditingkatkan menjadi *multi-user* berbasis *website* mulai akhir tahun 2011.

Dari studi pendahuluan yang dilakukan oleh peneliti, SIMPUS telah diterapkan dan digunakan dalam kegiatan pelayanan di Puskesmas Weru. Namun dalam pelaksanaanya masih ditemui berbagai masalah terkait aspek keamanan data dan pengelolaan akses pengguna. Salah satu permasalahan utama adalah *user* dan *password* tersimpan secara otomatis dalam sistem, sehingga pengguna dapat *login* tanpa memasukkan *user* dan *password* masing-masing pengguna. Selain itu, *password* tidak diganti secara berkala yang berpotensi meningkatkan risiko kebocoran data dan akses tidak sah

terhadap data informasi pasien. Kondisi tersebut menunjukkan bahwa mekanisme kontrol keamanan dalam Sistem Informasi Manajemen Puskesmas (SIMPUS) di Puskesmas Weru Kabupaten Sukoharjo masih perlu diperkuat agar sesuai dengan prinsip kerahasiaan, integritas, dan ketersediaan data sebagaimana tercantumkan dalam Permenkes N0. 24 Tahun 2022 tentang Rekam Medis Elektronik. Berdasarkan uraian dari permasalahan diatas peneliti melakukan penelitian dengan judul "Analisis Keamanan Data dan Informasi Kesehatan pada Sistem Informasi Manajemen Puskesmas (SIMPUS) di Puskesmas Weru Sukoharjo tahun 2025".

B. Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan, rumusan masalah penelitian ini adalah "Bagaimana keamanan data dan infromasi kesehatan pada sistem informasi manajemen puskesmas (SIMPUS) di Puskesmas Weru?.

C. Tujuan

1. Tujuan Umum

   Untuk menganalisis keamanan data dan informasi dalam SIMPUS di Puskesmas Weru Kabupaten Sukoharjo berdasarkan aspek *Confidential, Integrity*, dan *Availability* (CIA).

2. Tujuan Khusus
   a. Menganalisis keamanan data dan informasi pada SIMPUS berdasarkan aspek *Confidentiality* di Puskesmas Weru.
   b. Menganalisis keamanan data dan informasi pada SIMPUS berdasarkan aspek *Integrity* di Puskesmas Weru.
   c. Menganalisis keamanan data dan informasi pada SIMPUS berdasarkan aspek *Availability* di Puskesmas Weru.

D. Manfaat Penelitian

1. Manfaat Bagi Puskesmas

   Penelitian ini diharapkan dapat memberikan rekomendasi terkait

keamanan data pasien dalam SIMPUS.

2. Manfaat Bagi Akademik

   Penelitian ini dapat menjadi sumber informasi dan referensi ilmiah untuk pengembangan penelitian terkait sistem informasi kesehatan dan keamanan data.

3. Manfaat Bagi Mahasiswa

   Bagi mahasiswa sebagai peneliti, penelitian ini dapat memberikan pengalaman dan meningkatkan kemampuan analisis serta pengembangan kompetensi profesional di bidang kesehatan atau teknologi informasi.

E. Penelitian Terdahulu Sejenis

Penelitian terkait keamanan data telah banyak dilakukan sebelumnya terutama dalam konteks penerapan SIMRS dan rekam medis elektronik di rumah sakit. Penelitian – penelitian tersebut menjadi acuan dalam memahami praktik dan tantangan keamanan data. Berikut penelitian terdahulu sejenis yang relevan.

Table 1 Penelitian Terdahulu Sejenis

No	Peneliti	Judul Penelitian	Desain Penelitian	Variabel yang diteliti	Hasil
1.	Nurvianto & Jamroni (2017)	Analisis Keamanan Data Sistem Informasi di Puskesmas Pleret Bantul	Kualitatif deskriptif	Sistem Keamanan data server SIMPUS, pengetahuan dan sikap petugas	Tidak ada prosedur tetap keamanan server, pengamanan hanya melalui *password*. Pengetahuan petugas baik tapi pelaksanaan kurang, pengawasan minim, *backup* data dilakukan rutin
2.	Suhariyono , Ikawati, Afifah (20250	Analisis Aspek Keamanan Informasi Data Pasien	Deskriptif kualitatif	Aspek *confidentiality*, *integrity*, dan *availability* pada data rekam	Data aman dengan penggunaan *username* dan *password*,

		pada Rekam Medis Elektronik di UPT Puskesmas Karangploso		medis elektronik E-Puskesmas	pengeditan dan penghapusan data dibatasi oleh pihak berwenang, *backup* data aman, akses cepat dan tersedia kapan saja
3.	Widiyanti, Hastuti, Kusumawati (2022)	Tinjauan Keamanan Data Rekam Medis Elektronik pada Aplikasi SIMPUS di Puskesmas Tasikmadu Karanganyar	Deskriptif kualitatif	Keamanan data SIMPUS: *confidentiality*, *integrity*, dan *availability*	Keamanan data dengan *username* dan *password* sudah ada namun belum ada *automatic log off*, Penghapusan data dibatasi oleh admin, *Backup* data manual dan belum otomatis, akses data cepat dan tersedia
4.	Pradita, Kusumo, Rahmawati (2022)	Pentingnya Aspek Keamanan Informasi Data Pasien pada Penerapan RME di Puskesmas Botania	Kualitatif, wawancara	Kerahasian (*Confidentiality*), Integritas (*Integrity*), Ketersediaan (*Availability*)	E-Puskesmas belum memenuhi standar keamanan data (CIA Triad).
5.	Khoirunnisa (2025)	Tinjauan Keamanan Data Dan Informasi Sistem Informasi Manajemen Puskesmas (SIMPUS) Di Puskesmas Genuk Kota Semarang	Kualitatif, wawancara	Integrasi keamanan data dukungan manajemen, akses kontrol, ketahanan infrastruktur.	Keamanan terintegrasi tapi SOP *paperless* absen; *username* atau *password* ada namun rawan sharing, risiko mati listrik/internet ancam *availability* data.

Kebaruan penelitian ini berbeda dari penelitian terdahulu, penelitian ini fokus pada keamanan data dan informasi kesehatan dalam Sistem Informasi Manajemen Puskesmas (SIMPUS). Beberapa penelitian sebelumnya lebih fokus pada keamanan Rekam Medis Elektronik (RME) atau aplikasi E-Puskesmas dengan menilai aspek *Confidentiality*, *Integrity*, dan *Availability*. Penelitian ini secara khusus meneliti penerapan keamanan data pada SIMPUS di Puskesmas Weru, mencakup mekanisme kontrol akses pengguna, penggunaan *username* dan *password*, pembatasan hak akses, proses cadangan data, serta ketersediaan akses sistem untuk mendukung pelayanan kesehatan. Selain itu, penelitian ini tidak hanya mengkaji aspek teknis keamanan sistem, tetapi juga menggambarkan penerapan keamanan data dalam aktivitas layanan sehari-hari oleh petugas pengguna SIMPUS, sehingga memberikan gambaran tentang kondisi implementasi keamanan data SIMPUS secara langsung di lingkungan puskesmas.

BAB II
TINJAUAN TEORI

A. Tinjauan Pustaka

1. Puskesmas

a. Pengertian Puskesmas

Menurut Peraturan Menteri Kesehatan Republik Indonesia Nomor 19 Tahun 2024 Pusat Kesehatan Masyarakat yang selanjutnya disebut Puskesmas adalah fasilitas pelayanan kesehatan tingkat pertama yang menyelenggarakan dan mengkoordinasikan pelayanan kesehatan promotif, preventif, kuratif, rehabilitatif, dan paliatif di wilayah kerjanya. Upaya kesehatan adalah segala bentuk kegiatan atau serangkaian yang dilakukan secara terpadu dan berksinbungan untuk memelihara dan meningkatkan derajat kesehatan masyarakat. Kegiatan ini dapat dilakukan dalam bentuk promotif, preventif, kuratif, rehabilitatif dan paliatif oleh pemerintah pusat, pemerintah daerah, dan masyarakat.

b. Tugas Puskesmas

Menurut Peraturan Menteri Kesehatan Republik Indonesia Nomor 19 Tahun 2024 tentang Pusat Kesehatan Masyarakat tugas puskesmas adalah menyelenggarakan dan mengoordinasi pelayanan kesehatan promotif, preventif, kuratif, rehabilitatif, dan paliatif dengan mengutamakan promotif dan preventif di wilayah kerjanya. Tugas pokok puskesas antara lain :

1) Melaksanakan kebijakan kesehatan untuk mencapai tujuan pembangunan kesehatan di wilayah kerjanya.
2) Mengintegrasikan program yang dilaksanakan dengan pendekatan keluarga untuk meningkatkan jangkauan sasaran dan mendekatkan akses pelayanan kesehatan.
3) Pendekatan keluarga merupakan salah satu cara puskesmas mengintegrasikan program untuk meningkatkan jangkauan sasaran

dan mendekatkan akses pelayanan kesehatan di wilayah kerjanya dengan mendatangi keluarga.

Fungsi puskesmas mencakup penyelenggaraan pelayanan kesehatan primer di wilayah kerjanya. Selain itu, puskesmas juga menjadi tempat pelatihan bagi tenaga kesehatan, tempat program magang, serta tempat penelitian dan pngembangan di bidang kesehatan sesuai dengan peraturan perundang-undangan. Berikut fungsi puskesmas :

1) Puskesmas bertanggung jawab menyediakan dan mengoordinasi semua jenis pelayanan kesehatan, seperti promosi, pencegahan, pengobatan. Pemulihan, dan perawatan.
2) Puskesmas bertugas meningkatkan kualitas pelayanan kesehatan masyarakat dengan fokus pada promosi dan pencegahan.
3) Puskesmas membantu masyarakat meningkatkan kemampuan hidup sehat.
4) Puskesmas memberikan pelayanan kesehatan yang terpadu dengan sistem kelompok seperti manajemen, kesehatan ibu dan anak, kesehatan dewasa dan lansia, penanganan penyakit, kesehatan lingkungan, serta lintas kelompok.
5) Puskesmas wajib menggunakan sistem informasi kesehatan yang terpadu, termasuk catatan elektronik dan pelaporan data kesehatan untuk meningkatkan kualitas pelayanan kesehatan.
6) Puskesmas harus melakukan pengawasan dan evaluasi kinerja agar pelayanan yang diberikan sesuai dengan standar yang berlaku.

2. Sistem Informasi Manajemen Puskesmas (SIMPUS)

a. Pengertian Sistem Informasi Manajemen

Sistem Informasi Manajemen merupakan gabungan dari perangkat keras, perangkat lunak, infrastruktur, dan sumber daya manusia. Tujuanya adalah untuk mengumpulkan, mengolah, menyimpan, dan menyebarkan informasi yang dibutuhkan agar bisa mendukung fungsi manajerial dalam sebuah organisasi. Sistem Informasi Manajemen dirancang agar bisa memberikan informasi yang

benar, sesuai kebutuhan, dan tersedia tepat waktu sehingga para manajer bisa menggunakan informasi tersebut untuk pengambilan keputusan, merencanakan, mengendalikan, serta mengevaluasi berbagai hal (Andaria, 2024).

b. Pengertian Sistem Informasi Manajemen Puskesmas

Menurut Permenkes No 31 Tahun 2019 tentang Sistem Informasi Puskesmas (SIMPUS), merupakan sistem yang digunakan untuk memberikan informasi yang membantu proses pengambilan keputusan dalam memimpin pengelolaan Puskesmas agar tujuan kegiatan dapat tercapai. Sistem ini mencakup pengelolaan data dan informasi dari semua kegiatan pelayanan kesehatan masyarakat dan upaya kesehatan perorangan. SIMPUS dirancang sebagai bagian dari Sistem Informasi Kesehatan (SIK) nasional yang bertugas mengumpulkan, menyimpan, dan menyajikan data pelayanan kesehatan agar dapat digunakan sebagai dasar dalam perencanaan, pelaksanaan, pengawasan, dan evaluasi program puskesmas.

Sistem Informasi Manajemen Puskesmas (SIMPUS) adalah sistem yang menggunakan teknologi komputer dan dibuat khusus untuk membantu mengelola data dan informasi layanan kesehatan di puskesmas secara lengkap dan terpadu. Sistem ini mencakup kegiatan seperti mencatat dan menyimpan catatan medis pasien, pengelolaan persediaan obat, serta membuat laporan (Sari *et al.*, 2025).

c. Keamanan Data Pasien

Keamanan sistem informasi merupakan tindakan untuk melindungi sistem informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, pengecekan, pencatatan, atau perusakan yang ilegal. Tujuan utamanya adalah melindungi kerahasiaan, integritas, dan aksesibilitas data serta sistem informasi. Keamanan ini meliputi berbagai cara pencegahan untuk mengelakkan pelanggaran yang berkaitan dengan data, baik yang disimpan baik secara elektronik maupun secara fisik. Tujuan dari sistem keamanan informasi adalah

untuk menjamin bahwa data sensitif hanya bisa diakses oleh individu yang berwenang akses, dan tetap dilindungi dari pihak yang tidak berhak (Pardosi *et.al*, 2024). Perlindungan privasi pasien merupakan bagian penting dari kerahasiaan data dalam pengelolaan data medis. Ini menunjukkan bahwa data kesehatan pasien harus dijaga dengan ketat dan hanya dapat diakses oleh orang-orang yang berwenang dan pentingnya memahami informasi itu untuk memberikan perawatan yang benar. Selain melindungi privasi, penting juga untuk menjamin keselamatan data kesehatan pasien.

Sistem proteksi yang efektif perlu meliputi pengkodean data, pengawasan akses yang ketat, pencadangan rutin, dan langkah-langkah pemulihan bencana agar data medis tetap terlindungi dan dapat diakses saat dibutuhkan (Prawindha, 2025).

1) Definisi Keamanan data

   Keamanan data merupakan upaya untuk menjaga dan memastikan kerahasiaan informasi, integritas data, dan aksesbilitas data. Keamanan sistem informasi merupakan aspek yang sangat penting untuk menjamin keutuhan dan kualitas informasi yang akan dihasilkan. Data dan informasi harus dilindungi dari faktor kelalaian, kesengajaan dan masalah teknik serta etika yang diperkirakan dapat merusak dan menghambat proses distribusi (Gunawan, 2021).

2) Aspek Keamanan Data

   Menurut Permenkes No. 24 Tahun 2022 Pasal 29 menjelaskan bahwa keamanan data dan informasi memiliki tiga prinsip yaitu,

   a) Kerahasiaan (*Confidentiality*) 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.
   b) Integritas (*Integrity*) merupakan jaminan keakuratan data dan informasi yang ada dalam Rekam Medis Elektronik, perubahan

data hanya bisa dilakukan oleh orang yang benar-benar di beri hak akses.

c) Ketersediaan (*Availability*) merupakan jaminan keakuratan data dan informasi dalam Rekam Medis Elektronik dapat diakses dan digunakan oleh orang yang telah diberi izin oleh pimpinan Fasilitas Pelayanan Kesehatan.

Sedangkan menurut teori CIA Triad terdapat tiga elemen yang merupakan idikator keamanan informasi yang digunakan oleh para ahli untuk mengukur keamanan aplikasi(Hermawan, 2022). CIA Triad terdiri dari (*Confidentiality, Integrity, Availability*). Berikut pengertian dari elemen CIA Triad:

a) *Confidentiality* (Kerahasiaan)

Mengacu pada prinsip bahwa data harus dilindungi dan hanya dapat diakses oleh pihak yang berwenang melalui kontrol akses, enkripsi, dan autentikasi pengguna agar data tetap aman.

b) *Integrity* (Integritas)

Integritas memfokuskan pada jaminan keakuratan dan konsistensi data. Integritas menjaga agar data tidak berubah, dihapus, atau dimanipulasi tanpa izin dengan menggunakan mekanisme validasi, jejak audit, dan checksum sehingga infomasi tetap dapat diandalkan untuk pengambilan keputusan.

c) *Availability* (Ketersediaan)

Ketersediaan memastikan bahwa data dan sistem tersedia dan dapat diakses oleh pengguna yang berhak ketika diperlukan yang mencakup perlindungan dari gangguan sistem dan seragan *cyber*, serta penerapan cadangan dan pemulihan data untuk memastikan kelangsungan operasional.

3) Komponen Utama Keamanan Data SIMPUS

Komponen utama keamanan data SIMPUS terdiri dari tujuh elemen esensial yang saling terintegrasi (Safitri, 2025):

1. Kerahasiaan (*Confindentiality*)

Memastikan data pasien hanya dapat diakses oleh pihak yang berwenang.

2. Integritas (*Integrity*)

   Menjamin data agar tetap akurat dan tidak dapat diubah tanpa izin dan setiap perubahan data tercatat untuk menjaga keakuratan data.

3. Ketersediaan (*Availability*)

   Memastikan data dapat diakses kapan saja oleh pengguna yang sah.

4. Otentikasi

   Otentikasi memverifikasi identitas pengguna agar hanya pada pengguna sah yang dapat mengakses data menggunakan username atau *password*.

5. *Audit Trail*

   Melibatkan log aktivitas sistem dan pemantauan real-time pada data dan dapat dilacak bila diperlukan.

6. Enkripsi Data

   Melindungi data dalam penyimpanan dan transmisi dengan teknik enkripsi agar informasi tetap aman dari akses tanpa izin.

7. Kepatuhan dan kebijakan

   Mencakup standar ISO/IEC 27001, pelatihan staf tentang keamanan data, dan kebijakan retensi data.

4) Keamanan Jaringan

Keamanan jaringan melibatkan berbagai aspek dasar yang saling terhubung untuk melindungi sistem dari berbagai jenis ancaman, baik yang bersifat teknis maupun nonteknis. Secara menyeluruh, cakupan keamanan jaringan dapat dijelaskan sebagai berikut (Baharuddin, 2021):

1. Keamanan perangkat keras dan perangkat lunak

   Aspek ini memusatkan pada perlindungan infrastruktur fisik serta sistem aplikasi dari kemungkinan kerusakan, kehilangan,

pencurian, dan serangan *cyber* yang menyasar celah pada perangkat keras dan perangkat lunak.

2. Keamanan transmisi data

   Dimensi ini mengutamakan perlindungan data dalam proses pengiriman melalui jaringan. Pelaksanaan enkripsi, autentikasi, dan mekanisme perlindungan integritas data bertujuan untuk menghindari penyadapan, modifikasi, serta penyalahgunaan informasi oleh pihak yang tidak berwenang.

3. Pengelolaan akses dan identitas

   Pengelolaan akses bertujuan untuk menjamin bahwa hanya orang-orang dengan hak dan izin tertentu yang diperbolehkan mengakses sumber daya sistem. Mekanisme seperti otorisasi dan autentikasi diterapkan untuk mengatur hak akses sesuai dengan tanggung jawab dan peran pengguna.

4. Aturan dan langkah-langkah keamanan

   Aspek ini meliputi pembuatan regulasi, standar operasional, serta pedoman teknis yang berfungsi sebagai dasar untuk memastikan keamanan jaringan secara menyeluruh. Kebijakan yang terorganisir berperan sebagai pedoman bagi semua anggota organisasi dalam mengimplementasikan praktik keamanan.

5. Pengawasan dan identifikasi risiko

   Mencakup penerapan sistem deteksi intrusi, pencatatan log kegiatan, serta analisis risiko dini.

3. Strategi dan Perlindungan Data

Strategi perlindungan data mencakup berbagai cara untuk memastikan keamanan dan privasi data, seperti memperkuat keamanan sistem melalui penerapan standar seperti enkripsi data, deteksi aktivitas tidak biasa, serta regulasi dan standar keamanan, termasuk penerapan UU Perlindungan Data Pribadi (PDP) di Indonesia. Pendidikan dan peningkatan kesadaran masyarakat juga merupakan bagian dari strategi untuk memastikan bahwa hanya otoritas yang bisa mengakses data sensitif. Strategi lain mencakup

pengujian penetrasi secara berkala, penerapan solusi antivirus terbaru, dan penguatan kebijakan akses minimal bagi pengguna (Halim, Islam and Nasution, 2025). Berikut merupakan komponen kunci dalam pengendalian keamanan data:

a. Kontrol Akses dan Otentikasi

Kontrol akses dan Otentikasi merupakan elemen yang penting dalam melindungi data dan sistem informasi yang bertujuan untuk memastikan hanya orang yang berwenang yang bisa mengakses sumber daya tertentu. Manajemen Identitas dan Akses (IAM) berfungsi sebagai dasar utama dalam sistem ini yang meliputi proses identifikasi, otentikasi, otorisasi, dan audit akses pengguna untuk melindungi data dari akses yang tidak sah serta potensi ancaman *cyber* (Gemawaty *and* Yuliani, 2024).

b. Kriptografi

Kriptografi merupakan cabang ilmu yang krusial dalam melindungi kerahasiaan informasi dengan mengubah data asli yang dikenal sebagai *plaintext* menjadi suatu bentuk yang tidak terlihat yaitu *ciphertext* melalui proses enkripsi. Tujuan utama dari proses ini adalah untuk memastikan bahwa hanya individu yang memiliki kunci rahasia yang bisa mengembalikan *ciphertext* ke bentuk aslinya melalui deskripsi, sehingga data tetap terlindungi dari akses yang tidak sah (Halim, Islam and Nasution, 2025).

c. Kerangka Kerja Keamanan Informasi

Kerangka kerja keamanan informasi (*Information Security Framework*) adalah suatu sistem yang terdiri dari standar, kebijakan, prosedur, dan pedoman yang disusun secara terencana untuk membantu organisasi dalam mengenali, mengontrol, dan mengurangi risiko keamanan informasi. Kerangka ini berperan sebagai dasar konseptual dan operasional untuk melindungi aset digital organisasi, sembari memastikan bahwa prinsip kerahasiaan, integritas, dan ketersediaan data terjaga. Dengan demikian, kerangka kerja itu berfungsi sebagai

panduan strategis dalam merancang dan menerapkan sistem pengelolaan keamanan informasi yang menyeluruh dan berkelanjutan (ICRC, 2017).

4. Resiko dan Ancaman Informasi

Risiko dan ancaman informasi merupakan permasalahan krusial yang perlu ditangani secara terencana agar kelangsungan perlindungan data tetap terjaga. Risiko terhadap keamanan data dapat dibagi menjadi dua yaitu:

a. Ancaman dari luar

Ancaman dari luar adalah risiko yang muncul dari entitas di luar organisasi seperti serangan *cyber* (Peretasan, *Malware*, *Ransomware*), serangan *Distributed Denial of Service* (DDoS), pencurian data dan usaha untuk mengeksploitasi kelemahan sistem. Ancaman ini bersifat dinamis dan terus berubah seiring dengan kemajuan teknologi serta teknik penyerangan yang semakin maju. Oleh karena itu harus menerapkan standar keamanan dan metode perlindungan untuk mengidentifikasi dari ancaman tersebut (Sahira *et al.*, 2022).

b. Ancaman dari dalam

Ancaman dari dalam muncul dari dalam organsasi baik yang disengaja maupun tidak, seperti kesalahan manusia (*human error*), penyalahgunaan akses oleh staf, kebocoran data akibat pengawasan sistem yang kurang ketat atau sabotase internal. Ancaman internal dapat berisiko karena pelaku memiliki akses langsung ke sistem dan informasi. Oleh karena itu pengawasan akses, pelatihan keamanan, dan pemantauan aktivitas pengguna menjadi tindakan penting untuk menurunkan risiko ancaman dari dalam (Shelin, 2025).

Berikut beberapa risiko dan ancaman yang umum terhadap keamanan data pasien dalam SIMPUS (Suhariyono, 2025):

1) Risiko terkait pengelolaan *username* dan *password*, termasuk potensi penyalahgunaan dan kurangnya pergantian *password* secara berkala.
2) Ancaman perubahan data oleh administrator tanpa kontrol yang

memadai.

3) Risiko terkait penggunaan tanda tangan elektronik dan PIN yang belum optimal.
4) Ancaman terhadap data akibat kurangnya *backup* data yang memadai yang membuat data rentan terhadap kehilangan atau peretesan.
5) Risiko terkait penganturan pembatasan hak akses yang tidakkonsisten, sehingga membuka peluang akses data oleh pihak yang tidak berwenang.

5. Teori CIA Triad

CIA Triad adalah kerangka dasar dalam bidang keamanan informasi yang berperan sebagai pedoman dalam menilai sejauh mana suatu sistem atau aplikasi terlindungi. Konsep ini melibatkan tiga unsur utama, yaitu *Confidentiality, Integrity,* dan *Availability,* yang secara keseluruhan membangun fondasi perlindungan informasi. Berikut ini adalah penjelasan untuk setiap komponen tersebut (Moller, 2019):

a) *Confidentiality* (Kerahasiaan)

Kerahasiaan terkait dengan usaha untuk melindungi informasi agar tidak dapat diakses, diungkapkan, atau digunakan oleh pihak-pihak yang tidak berhak. Prinsip ini diterapkan melalui pengaturan akses, autentikasi dan otorisasi pengguna, serta penggunaan teknologi enkripsi untuk memastikan bahwa data tetap aman dari kemungkinan bocornya atau penyalahgunaannya.

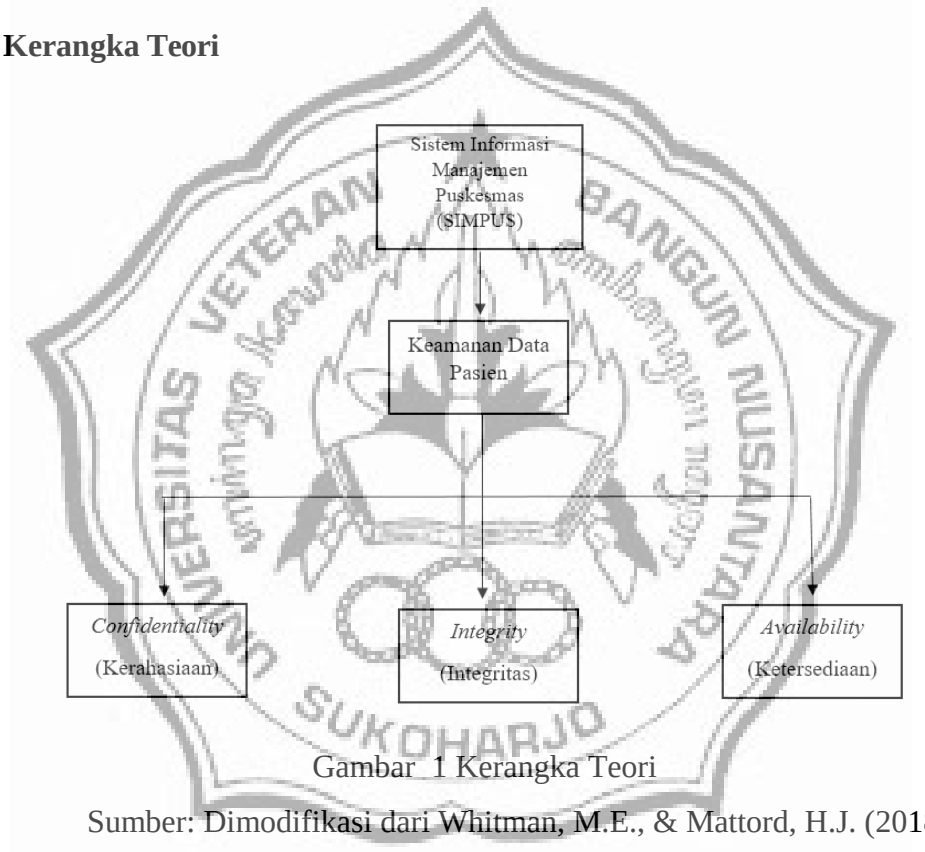
b) *Integrity* (Integritas)

Integritas menegaskan signifikansi menjaga akurasi, keutuhan, dan konsistensi data selama penyimpanan dan pengolahan. Prinsip ini bertujuan untuk menghindari terjadinya modifikasi, penghapusan, atau pemalsuan data tanpa izin dengan menerapkan mekanisme validasi, pencatatan jejak audit (*audit trail*), serta teknik verifikasi seperti *checksum*, sehingga informasi tetap dapat diandalkan sebagai dasar dalam pengambilan keputusan.

c) *Availability* (Ketersediaan)

Ketersediaan menekankan pada jaminan bahwa pengguna yang berwenang dapat mengakses sistem dan data setiap saat saat diperlukan. Penerapan prinsip ini meliputi perlindungan dari gangguan operasional, kerusakan sistem, dan serangan *cyber*, serta penyediaan mekanisme pemulihan data *(recovery*) dan pencadangan (*backup*) untuk memastikan kontinuitas layanan dan stabilitas operasional organisasi.

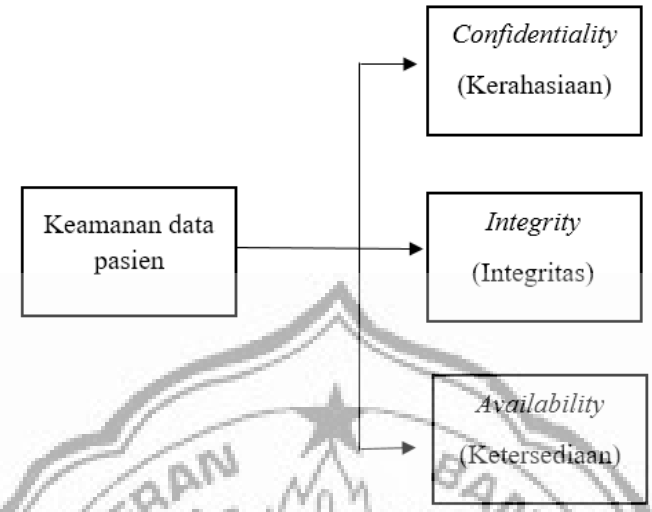
B. Kerangka Teori



Gambar 1 Kerangka Teori

Sumber: Dimodifikasi dari Whitman, M.E., & Mattord, H.J. (2018). *Principles of Information Security*.

C. Kerangka Konsep



Gambar 2 Kerangka Konsep

D. Pertanyaan Penelitian

1. Bagaimana keamanan data dan informasi kesehatan pada SIMPUS berdasarkan aspek *Confidentiality* di Puskesmas Weru?
2. Bagaimana keamanan data berdasarkan dan informasi kesehatan pada SIMPUS berdasarkan aspek *Integrity* di Puskesmas Weru?
3. Bagaimana keamanan data berdasarkan dan informasi kesehatan pada SIMPUS berdasarkan aspek *Availability* di Puskesmas Weru?