BAB I

PENDAHULUAN

A. Latar Belakang

Menurut Permenkes RI Nomor 24 tahun 2022 tentang Rekam medis elektronik menyatakan bahwa Rekam medis yang dibuat dengan menggunakan sistem elektronik yang diperuntukkan bagi penyelenggaraan rekam medis, dan terdapat ketentuan berkaitan dengan penyelenggaran Rekam Medis Elektronik yang terdapat pada permenkes tersebut yang harus diselenggarakan oleh rumah sakit meliputi registrasi pasien, pendistibusian data rekam medis elektronik, pengisian informasi klinis, pengolahan informasi Rekam medis elektronik, penginputan data untuk klaim pembiayaan, penyimpanan Rekam Medis Elektronik, penjaminan mutu rekam medis elektronik,dan trasfer isi Rekam Medis Elektronik.

Keterkaitan antara Sistem Informasi Manajemen Puskesmas dengan keamanan Sistem pada dasarnya sudah menjadi satu kesatuan dikarenakan didalam suatu Sistem Informasi Manajemen Puskesmas itu memiliki kerahasian bagi suatu organisasi. Keamanan Informasi merupakan suatu hal yang harus diperhatikan, masalah tersebut penting karena jika sudah Sistem Informasi dapat diakses oleh orang yang tidak berhak atau tidak bertanggung jawab.

Peraturan Arsip Nasional Republik Indonesia Nomor 15 Tahun 2021 tentang Sistem Manajemen keamanan informasi di Lingkungan Arsip

Nasional Indonesia, Keamanan informasi berati menjaga kerahasian,keutuhan dan ketersediaan informasi.

Penelitian oleh Pradita, Kusumo, dan Rahmawati (2020) menunjukkan bahwa keamanan data kesehatan dalam rekam medis elektronik harus memperhatikan kerahasiaan, integritas, dan ketersediaan. Penggunaan *username* dan *password*, *log off* otomatis, dan enkripsi data penting dalam menjaga kerahasiaan. Hasil Penelitian yang dilakukan oleh Saputra, Jamroni (2017) dengan hasil bahwa sistem keamanan dilakukan dengan penggunaan *password.* Namun pengetahuan petugas puskemas mengenai *system* keamanan sudah baik dilihat dari kepahaman petugas mengenai fungsi dan *password*.

Berdasarkan hasil survey pendahuluan di Puskesmas Jatiyoso bahwa SIMPUS 2023 masih menggunakan Rekam medis manual dan pada tahun 2024 telah terjadi perubahan rekam medis elektronik pada aplikasi SIMPUS Jojo ke SIMPUS Khanza, dalam implementasinya masih ditemukan kekurangan pada aspek keamanan *confidentiality* tidak terdapat *automatic log off* (ALO) akibatnya SIMPUS bisa di akses oleh orang lain yang tidak bertanggung jawab. Berdasarkan kendala pada latar belakang tersebut, maka penulis tertarik untuk melakukan penelitian dengan mengambil judul " Tinjauan Keamanan data Rekam Medis Elektronik pada aplikasi SIMPUS berdasarkan aspek *Confidentiality, Integrity, dan availability* Puskesmas Jatiyoso"

B. Perumusan Masalah

Bagaimana Keamanan data Rekam Medis Elektronik pada aplikasi SIMPUS di Puskesmas Jatiyoso?

C. Tujuan

1. Tujuan Umum

   Mengetahui keamanan data Rekam Medis Elektronik Pada aplikasi SIMPUS di Puskesmas Jatiyoso

2. Tujuan Khusus

   a. Mengetahui keamanan data SIMPUS berdasarkan aspek *confidentiality* di Puskesmas Jatiyoso

   b. Mengetahui Keamanan data SIMPUS berdasarkan aspek *integrity* di Puskesmas Jatiyoso

   c. Mengetahui Keamanan data SIMPUS berdasarkan aspek *availability* di Puskesmas Jatiyoso.

D. Manfaat

1. Bagi peneliti

   Peneliti diharapkan dapat menambah ilmu, wawasan dan pengalaman serta sebagai sarana untuk menerapkan ilmu yang diperoleh selama kuliah dengan yang ada di lapangan khususnya dalam bidang keamanan data

2. Bagi Puskesmas

   Manfaat peneliti untuk puskesmas diharapkan dapat menjadi salah satu

bahan masukan terkait keamanan SIMPUS sehingga dapat dijadikan pedoman dalam perbaikan sistem informasi manajemen puskesmas

3. Bagi Akademi

   Hasil penelitian ini diharapkan dapat menjadi referensi perpustakaan STIKes Mitra Husada Karanganyar dan dijadikan bahan bacaan atau referensi sebagai acuan penelitian sejenis berikutnya

BAB II

TINJAUAN PUSTAKA

A. Teori Yang Relevan

1. Puskesmas

Menurut undang-undang nomor 43 Tahun 2019, bab 1 pasal 1tentang pusat kesehatan masyarakat yang selanjutnya disebut Puskesmas adalah fasilitas pelayanan kesehatan yang memadukan upaya kesehatan masyarakat dan upaya kesehatan perseorangan tingkat pertama, serta memajukan kesehatan kesehatan dan mengutamakan upaya pencegahan bidang pekerjaannya. Puskesmas mempunyai tujuan pembangunan kesehatan yaitu menciptakan ruang kerja puskesmas yang sehat dengan komunitas yang :

a. Menunjukkan perilaku sehat yang meliputi kesadaran, kemamuan, dan kemampuan menjalani pola hidup sehat
b. Mampu memberikaan pelayanan kesehatan yang bermutu
c. Hidup dalam lingkungan sehat
d. Tercapainya tingkat kesehatan yang optimal bagi individu, kelompok keluarga, dan masyrakat

2. Rekam Medis Elektronik

Menurut Permenkes RI Nomor 24 Tahun 2022 Bab 2 pasal 5 dan 6 tentang Rekam Medis Elektronik merupakan salah satu subsistem dari sistem informasi pelayanan kesehatan yang terhubung dengan subsitem informasi lainnya di fasilitas pelayanan kesehatan, penyelenggaraan Rekam Medis elektronik dilakukan oleh unit kerja tersendiri atau

disesuaikan dengan kebutuhan dan kemampuan masing – masing fasilitas pelayanan kesehatan yang dilakukan sejak pasien masuk sampai pasien pulang, dirujuk, atau meninggal. Kegiatan pengelolaan Rekam Medis Elektronik sekurang – kurangnya meliputi :

a. Registrasi Pasie;
b. Pendistribusian data Rekam Medis Elektronik;
c. Pengisian Formulir kinis ; Pengelohan informasi Rekam Medis Elektronik ;
d. Penginputan data klaim pembiayaan
e. Penyimpanan Rekam Medis Elektronik
f. Penjaminan mutu Rekam Medis Elektronik
g. Transfer Rekam Medis Elektronik

3. Sistem Informasi Manajemen Puskesmas (SIMPUS)

a. Pengertian SIMPUS

Menurut Peraturan Menteri Kesehatan Nomor 31 Tahun 2019, SIMPUS merupakan salah satu sistem yang menyediakan informasi untuk mendukung proses pengambilan keputusan untuk mencapai tujuan kegiatan operasional puskesmas. Tujuan dari SIMPUS adalah mewujudkan penyelenggaran sistem informasi puskesmas yang terintergrasi, menjamin ketersediaan data dan informasi yang berkualitas, berkesinambungan, dan mudah diakses, serta meningkatkan kualitas pembangunan kesehatan di wilayah kerjanya melalui penguatan manajemen puskesmas. dalam melakasanakan

SIMPUS, Puskesmas memerlukan aplikasi, jaringan internet, dan *local area network* (LAN).

Ruang Lingkup SIMPUS menurut Barsella (2012) adalah :

1) Admin sistem (manajemen *user*)
2) Modul registrasi loket
3) Modul pelayanan poli umum
4) Modul pelayanan poli gigi
5) Modul pelayanan KIA
6) Modul pelayanan rawat inap
7) Modul pelayanan poli mata
8) Modul asset
9) Modul kepegawaian
10) Modul administrasi (percetakan surat keterangan / rujukan & laporan puskesmas)
11) Modul kegiatan eksternal / UKM (Posyandu lanjut usia, posyandu Anak, vaksinasi, kesehatan Lingkungan, pelayanan gizi, promosi kesehatan)

b. Keunggulan dan kelemahan SIMPUS

Menurut Barsella (2012), kelebihan penggunaan SIMPUS adalah :

1) Program ini didesain pada *windows* agar mudah digunakan dan membuat laporan yang menarik

2) Data terkait dibuat agar dapat dilakukan analisis untuk mendukung kebijakan pemerintahan daerah
3) Mengintegrasikan pelayanan dari area pendaftran ke area apotek untuk menimimalkan penggunaan kertas
4) Pengelolaan database yang dapat diakses secara kolektif sehingga membentuk database kedokteran daerah
5) Dapat dilihat dan dicetak berdasarkan kategori uang diinginkan atau gambaran keseluruhan masalah kesehatan
6) SIMPUS dapat digunakan dinaringan terpusat atau terdistribusi
7) Data pasien, laporan bulanan, dan data penyakit dapat dicari dengan mudah
8) Data dapat dicek sesuai permintaan

Adapun kelemahan atau kendala dalam menggunakan SIMPUS antara lain :

1) Kesulitan dalan pengumpulan data masih terdapat kabupaten/kota yang belum menyampikan laporan data puskesmas
2) Format pemasukan data mungkin tidak sesuai dengan format data negara
3) Laporan data tidak terkirim tepat waktu
4) Data terlalu lengkap
5) Sistem SIMPUS online lambat.

c. Evaluasi SIMPUS

Menurut Peraturan Menteri Kesehatan Republik Indonesia No. 13 Tahun 2019, dijelaskan bahwa evalusi SIMPUS dilaksanakan sebagai pembinaan dan pengawasaan terhadap impelentasi SIMPUS yang digunakan untuk

1) Meningkatkan mutu pelayanan SIMPUS
2) Mengembangkan SIMPUS yang efisien dan efektif

Sementara Menurut UU 46 tahub 2017 menyebutkan SIMPUS bagian dari elektronik kesehatan (E-Kesehatan) salah satu ayat di UU tersebut menjelaskan untuk mengetahui keberhasilan impelmentasi E-Kesehatan perlu dilakukan evaluasi setiap tahun dengan menilai pencapaian sasaran strategi, keluaran dari tiap ,isi, maupun masing – masing kegiatan yang ditetapkan. Pencapaian tujuan dan hambatan dalam penerapan e-health harus ditinju setiap tahun dan didiskusikan dengan seluruh pemangku kepentingan.

4. Keamanan Data dan Informasi

a. Pengertian Keamanan data dan Informasi

Keamanan data dan informasi mengacu pada langkah-langkah sistematis yang diambil untuk melindugi data agar tidak disusupi, dirusak atau disalah gunakan oleh individu baik didalam maupun diluar organisasi. Keamanan data dan informasi mencakup perlindungan data dari askes, perubahan, atau penghancuran yang tak sah dalam sistem,

serta melinuni sistem komputer dari seranan siber dan potensi riskio lainnya (Fadilla et al., 2022). Keamanan data dan nformasi sangat penting karena data adalah bahan baku informasi yang dapat berharga dan tidak dapat diganti, serta memilik nilai strateis bagi organsasi dan individu.

Informasi merupakan sumber daya yang sangat penting dan sangat berharga bagi kelangsungan hidup institusi organisasi, bisnis, keamanan nasional, serta interitas dan kedaulatan suatu negara. Informasi dapat disebarluaskan kepada publik melalui berbagai media, termasuk teks, gambar, audio, dan video. Tujuan utama manajemen informas adalah untuk menjaga kerahasiaan, interitas, dan aksesibilitas informasi.

Sistem Keamanan informasi mencakup serangkaian kebijakan, prosedur, dan langkah-langkah tekns yang dirancang untuk menggagalkan akses yang tidak sah atau melanggar hukum ke sistem infromasi. Seiring dengan kemajuan teknologi, sistem keamanan untuk teknologi informasi dapat ditingkatkan dan disempurnakan perangkat keras dan perangka lunak, jaringan komunikasi dan data (Mahfuz & Wasil, 2022).

1) Konsep Keamanan Data dan Informasi

Keamanan data dan informasi mengacu pada langkah-langkah yan**g** diambil untuk melindungi data dan informasi dari akses, gangguan, penyalahgunaan, penggunaan atau modifikasi yang tidak sah (Zen et al., 2023). Data dan informasi adalah aset yang sanar

berharga atau krusial dibagian bidang kehidupan, seperti pendidikan, bisnis dan pemerintahan. Keamanan data dan informasi meliputi tiga aspek utama, yang dikenal sebagai CIA triad : *Confdentiality* (kerahasiaan), *Integrity* (keaslian), *Availability* (Ketersediaan). *Confidentialitiy* berati melindungi data dari akses yang tidak sah, *Integrity* berati melindungi data dari modifikasi atau perubahan yang tidak sah, dan *Availability* berati melndungi data agar tetap dapat diakses dan digunakan secara efektif.

Keamana data dan Informasi juga didefiniskan sebagai upaya untuk meliundungi data dan informasi dari ancaman – ancaman yang dapat menyebabakan kerugian atau kerusakan. Data dan informasi adalah aset yang sangat berharga dan penting dalam berbagai aspek kehidupan ternasuk bisnis, pendidikan, dan pemerintahan. Oleh karena itu, keamana data dan informasi sangat diperlukan untuk melindungi data dan informasi dari ancama – ancaman yang dapat menyebabakan kerugian atau kerusakan.

2) Fungsi Keamanan data dan Informasi.

Keamanan data dan informasi memiliki fungsi yang sangat penting dalam melindungi data sensitif dan informasi rahasia dari kebocoran atau akses yang tidak sah (Munawar & Putri, 2020). Fungsi keamanan data dan informasi meliputi beberapa aspek :

(a) Kerahasiaan : Keamanan data dan informasi melindungi data dari akses yang tidak sah, memastikan bahwa hanya orang yang berwenang yang dapat mengakses informasi yang diperlukan.

(b) Integritas : Keamanan data dan informasi memastikan bahwa data tidak dapat diubah, dihapus, atau disalahgunakan oleh pihak yang tidak berwenang.

(c) Ketersediaan : Keamanan data dan informasi memastikan bahwa data tetap tersedia dan dapat diakses oleh orang yang berwenang ketika dibutuhkan.

(d) Kepatuhan : Keamanan data dan informasi memastikan bahwa data diproses dan disimpan sesuai dengan peraturan dan standar yang berlaku.

(e) Pencegahan Penggunaan Data yang Tidak Sah : Keamanan data dan informasi mencegah penggunaan data yang tidak sah atau kehilangan data, sehingga meminimalisir risiko kerugian bisnis dan reputasi

(f) Pengawasan Risiko : Keamanan data dan informasi memantau dan mengidentifikasi risiko yang terkait dengan data, sehingga dapat diambil tindakan untuk mengurangi atau menghilangkan risiko tersebut.

(g) Pengembangan dan Pemeliharaan Sistem Keamanan Keamanan data dan informasi melibatkan pengembangan. dan pemeliharaan sistem keamanan yang efektif untuk melindungi data dan

informasi.

(h) Pengawasan Jaringan : Keamanan data dan informasi melibatkan pengawasan jaringan untuk memastikan bahwa data tidak dapat diakses atau disalahgunakan oleh pihak yang tidak berwenang.

b. Menurut Hayaty (2020) tentang sistem keamanan

1) *Confidentiality* (Rahasia) berati menjaga kerahasian informasi dengan melakukan pembatasan akses sesorang yang paling umum dengan menggunakan enkripsi. Aspek ini bertujuan untuk :

a) Membatasi pengaksesan terhadapa informasi sesuai tingkat kerahasiaannya

b) Melindungi data/informasi agar tidak diketahui oleh pihak yang tidak berwenang.

2) *Integrity* (keaslian) berati manajemen bahwa data/informasi yang dimiliki terjaga keasliannya, tidak berubah tanpa pemilik informasi. *Integrity* merujuk pada tingkat kepercayaa terhadap suatu informasi. di dalam *integrity* terdapat 2 mekanisme pengamanan yaitu mekanisme *priventif* dan mekanisme detektif. Mekanisme *priventif* merupakan kontrol akses untuk menghalangi terjadinya modifikasi data. Sedangkan mekanisme deketif adalah untuk melakukan deteksi terhadap modifikasi yang telah dilakukan oleh orang lain. Aspek ini bertujuan untuk :

a) Melindungi data dan atau program agar tidak dimodifikasi tanpa izin oleh pihak yang tidak berwenang

b) Memberikan jaminan bahwa data/informasi yang ada pada *resource* dapat dipercayai.

3) *Availability* (ketersediaan) berhubungan dengan ketersediaan tersedia saat dibutuhkan oleh *user*, dan dapat dengan cepat diakses. Serangan yang paling lazim untuk jenis keamanan ini adalah *Distributed Denial of servies* (DDos). serangan ini memenuhi *resource* atau sumber informasi (*server*) dengan permintaan yang banyak atau permintaan diluar perkiraan sehingga *server* tidak dapat melayani permintaan lain atau bahkan *down.*

c. Menurut peraturan Menteri kesehatan No. 24 tahun 2022 tentang Rekam Medis Elektronik pasal 29 menjelaskan bahwa keamanan data dan informasi memiliki prinsip, yaitu :

1) *Confidentiality* (Kerahasiaan) kerahasiaan adalah menjamin keamanan data dan informasi dari campur tangan pihak internal dan eksternal yang tidak mempunyai akses, serta terlindunginya pengguna dan penyebaran data dan informasi dalam Rekam Medis Elektronik.

2) *Integrity* (integritas) integritas adalah keakuratan data dan informasi yang terkandung dalam Rekam Medis Elektronik. perubahan pada data hanya dapat dilakukan oleh mereka yang telah diberikan askes untuk melakukan perubahan tersebut.

3) *Availability* (Ketersediaan) Ketersediaan adalah jaminan bahwa data dan informasi yang terdapat dalam rekam medis elektronik

dapat diakses dan digunakan oleh individu yang hak aksesnya telah ditetapkan oleh pimpinan organisasi pelayanan kesehatan.

d. Menurut Sudra (2020), untuk membangun sistem pengamanan yang handal dan efektif, dibutuhkan tiga elemen program pengamanan informasi kesehatan yaitu:

1) Ketersediaan dokter dan personel lainnya akan dapat menjalankan tugasnya dengan lebih tenang dan percaya diri terkait dengan peraturan yang menjaga keamanan dan kerahasiaan data dalam berbagai informasi. Untuk menimalkan pengguna yang tidak berwenang mengekspioitasi sistem aktif yang telah ditinggalkan oleh pengguna lainnya yang berwenang, pastikan bahwa pengguna yang menggunakan sistem tersebut benar- benar pengguna yang sah/terutentikasi Anda perlu memastikan bahwa hal ini harus didukung dengan kemampuan untuk menggunkan *log-out* otomatis jika sistem tetap tidak aktif dalam jangka waktu tertentu atau jika pengguna yang berwenang mengakses sistem lagi melalui terminal kerja lain.

2) Integritas

Data terkait dengan informasi yang dihasilkan akan memiliki akurasi tinggi, sehingga petugas klinis, peneliti, dan petugas kesehatan lainnya menjadi yakin bahwa setiap tindakan yang direkomendasikan sudah berdasarkan data yang valid. integritas berati bahwa yang tersedia hanya dapat dimodifikasi atau diproses

untuk kebutuhan tertentu dan oleh penguna tertentu yang berwenang.

3) Ketersediaan informasi

Petugas pelayanan kesehatan akan lebih lancar menjalankan tugasnya bila informasi yang dibutuhkan selalu siap pada saat dibutuhkan dan ketersediaan sistem pelayanan dan prosedur pemulihan data untuk menjaga fungsinya dari gangguan dan manipulasi yang tidak sah. Sistem penyalinan data (*back up*) saat penting untuk mengantisipasi pemulihan sisitem secara cepat dan aman apabila terjadi kegagalan sistem.

B. Penelitian Yang Relevan

1. Pradita et.al., (2022) dengan judul " Pentingnya Aspek Keamanan Informasi Data pasien pada penerapan RME di Puskesmas" Menunjukkan bahwa hasilnya bahwa e-puskesmas belum memenuhi dapat diakses oleh pihak yang tidak berwenang. Selain ini, pencatatan elektronik rekam medis pada e-puskesmas perlu ditingkatkan terkait klaim pasien BPJS, Tim PKM merekomendasikan penggunaan *username* dan *password* individu, fitur *automatic log off* , pemblokiran akses jaringan, enkripsi data, dan integrasi dengan aplikasi BPJS kesehatan serta *back-up* data untuk mejaga keamanan data pasien. Dalam menjaga keamanan data kesehatan dan informasi dalam prinsip, yaitu kerahasiaan, aspek integritas, aspek ketersediaan.
2. Sofia, et.al., (2022) dengan penelitian yang berjudul "Analisis aspek

keamanan informasi pasien pada penerapan RKE di fasilitas kesehatan" dari hasil penelitianya menunjukkan bahwa aspek *privacy* pada penerapan rekam medis elektronik di fasilitas kesehatan, hal ini dilakukan dengan berbagai cara antara lain penggunaan nama pengguna dan kata sandi setiap pengguna. *Log- out otomatis.* serta pemblokiran akses melalui teknik enkripsi jaringan dan data. Pertimbangan integritas ketika menerapkan catatan kesehatan elektronik difasilitas kesehatan dilakukan dengan perubahan atau penghapusan data oleh adiminstator, aspek *availability* pada penerapan rekam medis elektronik difasilitas kesehatan dibuktikan dengan dapat terhubungnya sistem informasi kesehatan dengan perusahaan lainnya khususnya BPJS kesehatan, serta menggunakan proses *backup* data guna mengantisipasi peretusan data pasien

3. Dinasari ,A. (2023) dengan penelitian yang berjudul "Analisis keamanan Data pada penerapan Rekam Medis Elektronik di RSUD Dr. Adhyatma, MPH Provinsi Jawa Tengah" dari hasil penelitiannya ditinjau dari aspek *Confidentiality* sudah dilengkapi dengan pengguna *username* dan *password* dalam mengakses sisitem, hanya saja penerapan rekam medis elektronik pada SIMRS belum dibarengi dengan adanya automatic l*ogout* dan penggantian *password* secara berkala, dilihat dari aspek *integrity* masih belum terlaksana dengan sempurna. Hal ini disebabkan karena adanya batasan waktu pengeditan dalam melakukan perubahan ata pada rekam medis elektronik. Selajutnya dari aspek *availability* sudah berjalan dengan baik. Hal ini didukung dengan adanya proses pendistribusian rekam medis

elektronik yang sesuai dengan tujuan pengobatan pasien, akses dalam menggunakan rekam medis elektronik.

4. Widiyanti et,al., (2024) dengan judul " tinjauan keamanan data pada Rekam medis elektronik berdasarkan aspek *confidentiality, integrity* , dan *availability* di puskesmas Tasikmadu" menunjukan bahwa keamanan ata SIMPUS di tinaju dari aspek *Confidentiality*, dimana saat *user log-in* ke aplikasi SIMPUS sudah menggunakan hak *otentikasi* seperti memiliki *username* dan *password* disetiap bagian masing- masing sehingga tidak semua orang bisa *log-in*. Terkait kesalahan *enrty* bagian. Hanya saja SIMPUS belum di lengkapi dengan *automatic log off*. Selanjutnya keamanan data SIMPUS ditinjau dari aspek *integrity* dimana dalam aspek ini sudah dikatakan aman karena data saat diakses bisa diedit oleh pengguna pelayanan dibagiannya saja dan untuk penghapusan data hanya bisa dilakukan oleh admin SIMPUS, selajutnya ditinaju dari aspek *availability* sudah menunjang keamanan data karena saat data dibutuhkan pasti tersedia, data SIMPUS juga bisa diakses dimanapun asalkan *user* memiliki *otentikasi* seperti *username* dan *password*. Hanya saja SIMPUS belum dilengkapi *back-up* data otomatis tersimpan dikomputer selama 24 jam.
5. Penelitian Tiorentap et.al., (2020) dengan judul "Aspek Keamanan Informasi dalam penerapan Rekam Medis Elektronik di klinik *medical check up* MP" menunjukkan bahwa berdasarkan hasil observasi di klinik Medical *Check -Up* MP ditemukan ketidaksesuaian prinsip keamanan

sistem infomasi, yaitu pertukaran informasi yang berkelanjutan antar pengguna mengenai ID pengguna dan kata sandi selain itu, satu ID pengguna sering kali digunakan oleh banyak orang tentu saja, jika terjadi kesalahan ketik dsn pelakunya sulit didentifikasi, hal ini bisa berakibat fatal. Jika hal ini terus berlanjut, dikhawatirkan informasi tersebut akan dimanfaatkan oleh pihak yang tidak bertanggung jawab berdasarkan penjelasan di atas,saya ingin mempertimbangkan aspek keamanan informasi ketika memperkenalkan rekam medis elektronik.

BAB III

METODE PENELITIAN

A. Rancangan Penelitian

Jenis penelitian ini adalah penelitian deskriptif dengan pendekatan kualitatif, dimana penelitian ini bertujuan untuk menggambarkan tentang keamanan data rekam medis elektronik pada aplikasi SIMPUS berdasarkan aspek *confidentiality*, *integrity*, dan *availability* di Puskesmas Jatiyoso.

B. Waktu Dan Tempat Penelitian

1. Waktu Penelitian

   Penelitian ini dilaksanakan mulai bulan Febuari sampai Maret 2025

2. Tempat Penelitian

   Penelitian ini dilaksanakan di Puskesmas Jatiyoso khususnya dibagian pendaftaran Rekam medis rawat jalan.

C. Subyek dan Obyek Penelitian

1. Subyek

   Subyek dari penelitian merupakan 3 petugas pengguna SIMPUS yaitu petugas pendaftaraan Rekam Medis, Perawat, dan Kepala Rekam medis

2. Obyek

   Objek dalam penelitian ini adalah Aplikasi sistem informasi manajemen Puskesmas (SIMPUS) bagian Rekam medis Rawat jalan Puskesmas Jatiyoso

D. Definsi Konsep

Tabel 3.1
Definsi Konsep

No	Konsep	Definsi
1.	*Confidentiality* (Kerahasiaan)	Menjamin keamanan data dan infromasi dari gangguan pihak lain yang tidak memiliki hak akses/otorisasi dan pemastian terhadaap pengguna yang sah/otentikasi, sehingga data dan informasi yang ada dalam SIMPUS terlindungi pengguna dan penyebarannya
2.	*Integrity* (Integritas)	Menjamin data akurat dengan cara memberikan batasan sistem yang terdapat dalam SIMPUS, dan informasi tersebut hanya dapat dibuat oleh orang yang mempunyai batasan sistem dapat di edit pada saat oleh petugas yang terkait dalam pelayanan pasien.
3.	*Availability* (Ketersediaan)	Menjamin data dan informasi yang ada dalam SIMPUS dapat diakses saat dibutuhkan atau realtime oleh perawat manajemen atau pelayanan pasien dan tersedia saat dibutuhkan

E. Instrumen dan Cara Pengumpulan Data

1. Instumen Penelitian

   a. Pedoman wawancara

      Pedoman wawancara penelitian ini menggunakan daftar pertanyaan tentang keamanan SIMPUS di Puskesmas Jatiyoso.

   b. Pedoman Observasi

      Pedoman observasi yang digunakan pada penelitian ini adalah daftar pengamatan yang dibutuhkan dalam penelitian tentang pelaksanaan perlindungan keamanan data pada SIMPUS di Puskesmas Jatiyoso

c. Alat Perekam

Alat yang digunakan untuk merekam hasil wawancara setelah mendapatkan izin dari setiap respoden yang akan di wawancara.

2. Cara pengumpulan data

a. Wawancara

Pada penelitian ini wawancara yang dilakukan adalah wawancara terstruktur , peneliti daftar pertanyaan yang tersusun secara terperinci kepada petugas pendaftraaan rekam medis, perawat, dan kepala rekam medis.

b. Observasi

Cara pengumpulan data dalam penelitian ini menggunakan metode observasi, yaitu dengan mengamati mengenai keamanan data rekam medis elektronik pada aplikasi SIMPUS berdasarkan aspek *confidentiality*, *integrity* dan *availability* di Puskesmas Jatiyoso

F. Keabsahan Data

Triangulasi adalah metode yang digunakan dalam penelitian kualitatif untuk memeriksa dan menetapkan *validitas* dengan menganalisa dari berbagai *perspektif*. *Validitas* dalam penelitian kualitatif dilihat berdasarkan akurasi sebuah alat ukur yaitu instrumen.. Kelebihannya adalah bisa mendapatkan akurasi data. Menurut Sugiyono (2015) triangulasi data merupakan teknik pengumpulan data yang sifatnya menggabungkan berbagai data dan sumber

yang telah ada. Maka terdapat triangulasi sumber, triangulasi teknik pengumpulan data dan triangulasi waktu.

1. Triangulasi Sumber

   Triangulasi sumber untuk menguji *kredibilitas* suatu data dilakukan dengan cara melakukan pengecekan pada data yang telah diperoleh dari berbagai sumber data seperti hasil wawancara, arsip, maupun dokumen lainnya.

2. Triangulasi Teknik

   Triangulasi teknik untuk menguji kredibiltas suatu data dilakukan dengan cara melakukan pengecekan pada data yang telah dipeoleh dari sumber yang sama menggunakan teknik yang berbeda. misalnya data yang diperoleh dari hasil observasi, kemudian dicek dengan wawancara.

3. Triangulasi Waktu

   Waktu dapat mempengaruhi kredibilitas suatu data. data yang diperoleh dengan teknik wawancara dipagi hari pada saat narasumber masih segar biasanya akan menghasilkan data yang lebih valid. Untuk itu pengujian kredibilitas suatu data harus dilakukan pengecakan dengan observasi, wawancara dan dokumentasi pada waktu atau situasi yang berbeda sampai mendapatkan data yang kredibel.

G. Teknik Analisis dan Pengolahan Data

1. Pengolahan Data

   a. Reduksi Data

      Redukasi data adalah merangkum, memilih hal-hal yang pokok,

memfokuskan pada hal-hal yang penting dicari tema dan polanya Kegiatan menggolongkan ke dalam setiap permasalahan melalui uraian singkat, membuang yang tidak perlu mengenai keamanan data rekam medis elektronik pada aplikasi SIMPUS berdasarkan aspek *confidentiality*, *integrity* dan *availability* di Puskesmas Jatiyoso

b. Penyajian Data

Proses penyajian data, data yang diperoleh tersusun sesuai pola hubungan sehingga mudah dipahaim. Dalam penelitian ini data yang disajikan dalam bentuk narasi

c. Penarikan kesimpulan

Penarikan kesimpulan dilakukan mulai dari data yang dikumpulkan kemudian diambil kesimpulan secara umum mengenai keamanan data yang terbagai menjadi aspek *confidentialitiy*, *integrity*, dan *availability*.

2. Analisis Data

Penelitian ini di secara analisis deskriptif yaitu tentang menganalisis dan memaparkan hasil-hasil penelitian yang sesuai dengan keadaan sebenarnya mengenai keamanan data rekam medis elektronik pada aplikasi SIMPUS berdasarkan *confidentiality*, *integrity*, dan *availablity* di Puskesmas Jatiyoso.

H. Jadwal Penelitian

Tabel 3.2
Jadwal Penelitian Penyusunan Karya Tulis Ilmiah

No.	Kegiatan	Januari				Februari				Maret				April				Mei			
		I	II	III	IV	I	II	III	IV	I	II	III	IV	I	II	III	IV	I	II	III	IV
1.	Penyusunan Proposal																				
2.	Survei Pendahuluan																				
3.	Pengambilan Data																				
4.	Penyusunan Hasil																				
5.	Seminar Hasil																				
6.	Perbaikan																				
7.	Ujian KTI																				
8.	Penyempurnaan																				
9.	Pengumpulan KTI																				