BAB I
PENDAHULUAN

A. Latar Belakang

Fasilitas Pelayanan Kesehatan adalah suatu tempat yang digunakan untuk menyelenggarakan upaya pelayanan kesehatan, baik promotif, preventif, kuratif maupun rehabilitatif yang dilakukan oleh pemerintah, pemerintah daerah atau masyarakat. Berdasarkan PERMENKES No.43 Tahun 2019 Tentang Pusat Kesehatan Masyarakat (PUSKESMAS) adalah fasilitas pelayanan kesehatan yang menyelenggarakan upaya kesehatan masyarakat dan upaya kesehatan perseorangan tingkat pertama, dengan lebih mengutamakan upaya promotif dan preventif di wilayah kerjanya. untuk mewujudkan pusat kesehatan masyarakat yang efektif, efisien, dan akuntabel dalam penyelenggaraan pelayanan kesehatan tingkat pertama yang bermutu dan berkesinambungan dengan memperhatikan keselamatan pasien dan masyarakat, dibutuhkan pengaturan organisasi dan tata hubungan kerja pusat kesehatan masyarakat (Fitrina, 2022).

Keamanan dokumen rekam medis menyangkut dalam bahaya dan kerusakan dokumen rekam medis sendiri. Adapun aspek dari kerusakan yang dimaksud meliputi aspek fisik, aspek kimiawi, aspek biologis serta pencurian. Aspek fisik adalah kerusakan dokumen seperti kualitas kertas dan tinta yang disebabkan oleh sinar matahari, hujan, banjir, panas dan kelembaban. Aspek kimiawi adalah kerusakan dokumen yang disebabkan oleh makanan, minuman, dan bahan-bahan kimia. Aspek biologis adalah kerusakan dokumen yang disebabkan oleh tikus, kecoa dan rayap (Wijayanti, 2024).

Seiring perkembangan teknologi, puskesmas juga membangun sistem informasi yaitu Sistem Informasi manajemen Puskesmas atau biasa disebut SIMPUS. SIMPUS adalah suatu tatanan yang menyediakan informasi untuk membantu proses pengambilan keputusan dalam melaksanakan manajemen Puskesmas untuk mencapai sasaran kegiatanya. SIMPUS sangat berguna bagi proses pelayanan yang ada di puskesmas, dan mempermudah saat membuat

laporan dimana data yang dikumpulkan berasal dari SIMPUS (Amaliyah, 2024).

Keberadaan informasi elektronik atau dokumen elektronik mengikat dan diakui sebagai alat bukti yang sah untuk memberikan kepastian hukum terhadap penyelenggaraan sistem elektronik dan transaksi elektronik, terutama dalam pembuktian dan hal yang berkaitan dengan perbuatan hukum yang dilakukan melalui sistem elektronik. Rekam medis dapat dipergunakan sebagai alat pembuktian sesuai yang tertulis dalam Pasal 1866 KUHAP perdata dan pasal 184 KUHAP (Lakada, 2024) .

Ketentuan Pasal 1866 KUHP Perdata menyebutkan, Alat bukti meliputi: bukti tertulis; bukti saksi; persangkaan; pengakuan; dan sumpah. Sedangkan Pasal 184 Ayat (1) KUHAP, alat bukti yang sah dalam hukum pidana: (1) Keterangan saksi; (2) Keterangan ahli; (3) Surat; (4) Petunjuk; (5) Keterangan terdakwa. Kewajiban seorang perekam medis adalah membuat rekam medis sebaik mungkin. Salah satu alasannya adalah untuk pembuktian, rekam medis yang dibuat secara kronologis baik akan menjadi bukti kuat dalam pengadilan. Kerahasian yang menyangkut riwayat penyakit pasien yang terdapat pada rekam medis harus wajib dijaga oleh tenaga kesehatan yang melakukan praktik kedokteran. Rekam medis yang dibawa kepengadilan harus memenuhi syarat sebagai berikut rekam medis tidak ditulis dengan pensil, tidak ada penghapusan, coretan, ralat hanya dapat dilakukan pada saat itu juga dan diberi paraf, tulisan jelas dan terbaca, ada tanda tangan dan nama petugas, ada tanggal dan waktu pemeriksaan maupun tindakan, ada lembar persetujuan tindakan medis (Mokosolang, 2023).

Sistem keamanan terdiri dari beberapa aspek, diantaranya yaitu *privacy* atau *confidentiality* yang berhubungan dengan kerahasiaan data pasien, *integrity* berkaitan dengan perubahan data informasi, autenthication berhubungan dengan akses terhadap informasi, *avaliability* atau ketersediaan merupakan aspek yang menekankan pada ketersediaan informasi data pasien apabila dibutuhkan oleh pihak terkait, acces control adalah aspek yang menekankan pada cara pengaturan akses terhadap informasi dan yang terakhir adalah non-repundation berkaitan dengan suatu transaksi atau perubahan informasi (Alia, 2024).

Pentingnya Keamanan Data Pasien dalam Implementasi Rekam Medis Elektronik (RME). Perlindungan Informasi Sensitif Data pasien mencakup informasi yang sangat sensitif, seperti riwayat kesehatan, diagnosa, pengobatan, dan data pribadi lainnya. Keamanan data memastikan bahwa informasi ini tidak jatuh ke tangan yang salah dan digunakan untuk tujuan yang tidak sah. Kepatuhan Hukum dan Regulasi Banyak negara memiliki regulasi ketat yang mengatur perlindungan data pasien, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia. Implementasi keamanan yang baik memastikan bahwa fasilitas kesehatan mematuhi hukum dan menghindari sanksi atau denda (Jaeni, 2024).

Meningkatkan Kepercayaan Pasien, pasien lebih cenderung mempercayai fasilitas kesehatan yang dapat menjaga kerahasiaan data mereka. Keamanan data yang kuat menciptakan rasa aman bagi pasien, meningkatkan kepercayaan terhadap layanan kesehatan yang diberikan dan Pencegahan Pelanggaran Data / Pelanggaran data dapat mengakibatkan kerugian besar, baik secara finansial maupun reputasi. Dengan menerapkan langkah-langkah keamanan yang kuat, fasilitas kesehatan dapat mencegah insiden tersebut, melindungi diri dari kerugian dan biaya pemulihan (Arimbi, 2024).

Memastikan Keberlangsungan Layanan Keamanan data yang baik juga melindungi dari gangguan operasional akibat serangan *siber*, seperti *ransomware*, yang dapat mengakibatkan *downtime* sistem dan mengganggu layanan kesehatan. Dukungan untuk Keputusan Klinis Keamanan data pasien memastikan bahwa informasi yang digunakan untuk pengambilan keputusan klinis adalah akurat dan terpercaya. Data yang aman dan tidak terkompromi mendukung kualitas layanan kesehatan yang lebih baik. Fleksibilitas dan Aksessibilitas Dengan data yang aman, staf medis dapat mengakses informasi pasien dengan lebih fleksibel dan cepat, tanpa mengorbankan keamanan. Ini mendukung efisiensi dalam pelayanan dan pengambilan keputusan medis (Pardosi, 2024).

Keamanan data pasien bukan hanya masalah teknis, tetapi juga melibatkan kebijakan, prosedur, dan kesadaran dari seluruh pihak yang terlibat. Metode yang sering digunakan untuk menganalisis keamanan data pasien pada sistem RME adalah *CIA Triad* (*Confidentiality*, *Integrity*, *Availability*). Aspek yang termasuk dalam *CIA Triad* yaitu *Confidentiality* (Kerahasiaan) data pasien hanya dapat diakses oleh pihak yang berwenang, seperti dokter dan tenaga kesehatan yang memiliki izin , *integrity* (Integritas) data medis tidak boleh diubah atau dimanipulasi oleh pihak yang tidak berwenang, sehingga keakuratan dan keandalannya tetap terjaga, *Availability* (Ketersediaan) sistem RME harus selalu tersedia sehingga dapat diakses oleh pengguna yang berhak ketika dibutuhkan, tanpa gangguan teknis yang signifikan *Health Insurance Portability and Accountability Act* (HIPAA) HIPAA adalah regulasi yang banyak dijadikan referensi dalam keamanan data kesehatan (Hammam, 2024).

Berdasarkan hasil studi pendahuluan yang telah dilakukan di Puskesmas Gatak Sukoharjo, didapatkan informasi bahwa di Puskesmas Gatak sudah mulai menerapkan Rekam Medis Elektronik sejak tahun 2018. Dalam pengimplementasian rekam medis elektronik dijelaskan bahwa: Hak akses komputer diberikan kepada semua petugas pelayanan kesehatan Puskesmas Gatak dengan menggunakan *id user* dan *password* yang sama, serta akses ini kenyataannya ditempel di depan komputer bagian pendaftaran. Puskesmas Gatak belum menggunakan *firewall* yang berfungsi untuk mencegah akses yang tidak sah. Puskesmas Gatak belum menggunakan aplikasi perlindungan terhadap serangan seperti *Denial-Of-Service (DoS)* dan hanya menggunakan *password* komputer untuk perlindungan data pasien. Puskesmas Gatak belum menggunakan sistem enkripsi untuk melindungi data pasien dari akses *ilegal*. Puskesmas Gatak belum menggunakan *autentifikasi* ganda (2FA) untuk mengakses sistem data pasien. Sudah dilakukan pencadangan (*backup)* secara rutin tetapi belum ada aplikasi tambahan untuk menghindari kehilangan data akibat serangan *cyber*. Di Puskesmas Gatak sering terjadi dobel input data pasien, sebagai contoh bahwa 1 NIK berada pada 2 identitas nama yang berbeda,

pada studi pendahuluan tersebut dapat menimbulkan resiko kebocoran informasi data pasien.

Berdasarkan latar belakang tersebut penulis mengambil judul penelitian "Analisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik di Puskesmas Gatak".

B. Rumusan Masalah

Rumusan masalah pada penelitian ini adalah "Bagaimana aspek keamanan data pasien dalam implementasi rekam medis elektronik di Puskesmas Gatak Sukoharjo ?"

C. Tujuan Penelitian

1. Tujuan Umum

   Menganalisis aspek keamanan data pasien dalam implementasi Rekam Medis Elektronik di Puskesmas Gatak.

2. Tujuan Khusus
   1) Menganalisis penerapan aspek *confidential* pada Rekam Medis Elektronik di Puskesmas Gatak.
   2) Menganalisis penerapan aspek *integrity* pada Rekam Medis Elektronik di Puskesmas Gatak.
   3) Menganalisis penerapan aspek *avaliability* pada Rekam Medis Elektronik di Puskesmas Gatak.

D. Manfaat Penelitian

1. Manfaat Praktis
   a. Bagi Puskesmas

      Dapat digunakan sebagai bahan evaluasi dan pertimbangan bagi puskesmas dalam menyusun kebijakan dan Meningkatkan Kepercayaan Pasien Ketika pasien mengetahui bahwa data mereka dilindungi dengan baik, tingkat kepercayaan mereka terhadap layanan Puskesmas meningkat, yang dapat memperkuat hubungan antara pasien dan penyedia layanan kesehatan.

b. Bagi Peneliti

Dapat menambah pengetahuan, pengalaman dan wawasan yang berhaga secara langsung di Puskesmas dengan menerapkan teori yang dperoleh peneliti di institusi pendidikan.

2. Manfat Teoritis

a. Bagi Institusi Pendidikan

Dapat menjadi bahan masukan dalam pembelajaran di bidang ilmu rekam medis dan manajemen informasi kesehatan serta dapat meningkatkan pengetahuan tentang aplikasi SIMPUS pada aspek keamanan data pasien dalam implementasi rekam medis elektronik.

b. Bagi peneliti lain

Dapat digunakan sebagai acuan dalam memperoleh materi aspek keamanan data pasien dalam implementasi rekam medis elektronik untuk kelanjutan peneliti yang relevan

BAB II
TINJAUAN TEORI

A. Tinjauan Pustaka

1. Puskesmas

a. Definisi Puskesmas

Puskesmas (Pusat Kesehatan Masyarakat) adalah unit pelayanan kesehatan yang bersifat primer dan berfungsi sebagai pusat penyelenggaraan upaya kesehatan masyarakat, serta sebagai tempat pertama kali bagi masyarakat untuk mendapatkan layanan kesehatan. Puskesmas bertujuan untuk memberikan pelayanan kesehatan yang terjangkau dan berkualitas, terutama bagi masyarakat di wilayah tertentu, baik di daerah perkotaan maupun pedesaan (Aprilia, 2024) .

b. Tugas dan Fungsi Puskesmas

1) Pelayanan Kesehatan Masyarakat: Melakukan upaya promotif (promosi kesehatan) dan *preventif* (pencegahan penyakit) seperti imunisasi, penyuluhan kesehatan, dan program kesehatan lingkungan.
2) Pelayanan Kesehatan Perorangan: Memberikan pelayanan kesehatan dasar kepada individu, seperti pemeriksaan kesehatan, pengobatan, dan rujukan jika diperlukan.
3) Pengelolaan Kesehatan Wilayah: Puskesmas bertanggung jawab atas kesehatan masyarakat di wilayah kerjanya, termasuk pengumpulan data dan pemantauan kondisi kesehatan masyarakat.
4) Pelayanan *Kuratif*: Menangani pengobatan dan perawatan individu yang sakit.
5) Pelayanan *Rehabilitatif*: Memberikan layanan pemulihan kesehatan bagi pasien.
6) Pelayanan *Promotif* dan *Preventif*: Meningkatkan kesehatan masyarakat dan mencegah terjadinya penyakit (Sudarman, 2023).

Puskesmas juga sering menjadi pelaksana program kesehatan pemerintah, seperti program kesehatan ibu dan anak, pengendalian penyakit menular, serta

gizi masyarakat. Puskesmas dikelola oleh pemerintah daerah dan merupakan bagian penting dari sistem pelayanan kesehatan di Indonesia, dengan tujuan utama meningkatkan derajat kesehatan masyarakat secara keseluruhan (Gurning, 2024).

2. Rekam Medis Elektronik (RME)

a. Pengertian Rekam Medis Elektronik (RME)

Menurut Peraturan Menteri Kesehatan Republik Indonesia (Permenkes RI) Nomor 269/Menkes/Per/III/2008 dinyatakan bahwa:"Rekam medis adalah berkas yang berisi catatan dan dokumen tentang identitas pasien, hasil pemeriksaan, pengobatan, serta tindakan dan pelayanan lain yang telah di berikan kepada pasien (Hapsari, 2024).

Electronic Medical Record (EMR) atau rekam medik elektronik yang merupakan bagian dari *Eletronic Health Record* (EHR) telah banyak digunakan di berbagai rumah sakit di berbagai belahan dunia untuk menggantikan atau melengkapi rekam medik berbentuk kertas. Rekam medis elektronik adalah versi dari rekam medis kertas yang dibuat menjadi elektronik, yang memindahkan catatan-catatan atau formulir yang tadinya ditulis diatas kertas kedalam bentuk elektronik. Rekam medis elektronik tidak disertai dengan peringatan (*warning*), kewaspadaan (*alertness*) serta tidak memiliki system penunjang keputusan (*Decision Suport System*) (Sriwati, 2021).

b. Strandar Implementsi Rekam Medis Elektronik (RME)

Standar implementasi Rekam Medis Elektronik (RME) dirancang untuk memastikan bahwa data pasien dikelola dengan aman, efisien, dan sesuai dengan regulasi. Berikut adalah beberapa standar yang umumnya diterapkan dalam implementasi RME (Wibowo, 2024):

1) Standar Keamanan Data

a) Enkripsi Data**:** Data pasien harus dienkripsi saat disimpan dan saat ditransmisikan untuk melindungi dari akses tidak sah.

b) Autentikasi dan Otorisasi: Sistem harus mengadopsi autentikasi yang kuat (misalnya, penggunaan *password*, biometrik, atau token) untuk

memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses data.

c) Pengendalian Akses**:** Hanya personal tertentu yang diberi izin untuk mengakses informasi tertentu, berdasarkan peran dan tanggung jawab mereka.

2) Kepatuhan terhadap Regulasi

a) HIPAA (*Health Insurance Portability and Accountability Act*) di AS dan GDPR (*General Data Protection Regulation*) di Eropa adalah contoh regulasi yang menetapkan standar perlindungan data pasien.

b) Di Indonesia, implementasi harus sesuai dengan Undang-Undang Perlindungan Data Pribadi (UU PDP)**.**

3) Standar Interoperabilitas

a) HL7 (*Health Level Seven*): Standar internasional untuk pertukaran, integrasi, berbagi, dan pengambilan informasi elektronik kesehatan.

b) FHIR (*Fast Healthcare Interoperability Resources*): Standar yang lebih baru yang memungkinkan pertukaran data kesehatan dengan cara yang lebih fleksibel dan cepat.

c) DICOM (*Digital Imaging and Communications in Medicine*)**:** Standar untuk penyimpanan dan transmisi gambar medis.

4) Standar Kualitas Data

a) Data *Integrity*: Memastikan bahwa data yang dimasukkan ke dalam sistem adalah akurat, lengkap, dan dapat diandalkan.

b) Data *Consistency*: Informasi pasien harus konsisten di seluruh sistem, baik saat diakses oleh berbagai departemen atau fasilitas kesehatan yang berbeda.

5) Standar Pelaporan dan Audit

a) Audit Trail: Sistem harus mencatat semua aktivitas yang dilakukan dalam sistem, seperti siapa yang mengakses data, kapan, dan apa yang diakses, untuk tujuan audit dan keamanan.

b) Pelaporan Insiden: Ada mekanisme pelaporan untuk setiap insiden keamanan atau pelanggaran data yang terjadi.

6) Standar Pengelolaan Risiko

a) Analisis Risiko**:** Melakukan evaluasi rutin terhadap potensi risiko keamanan dan privasi, serta mengambil langkah-langkah untuk memitigasi risiko tersebut.

b) *Contingency Planning***:** Menyediakan rencana darurat untuk memastikan data tetap aman dan layanan tetap berjalan dalam situasi darurat atau bencana (Wibowo, 2024).

Implementasi RME yang memenuhi standar ini akan membantu fasilitas kesehatan dalam menyediakan layanan yang lebih aman, efisien, dan berkualitas, serta memastikan perlindungan data pasien.

3. Keamanan Data Pasien

a. Definisi Kemanan Data Pasien dalam Konteks RME:

Keamanan data dalam konteks Rekam Medis Elektronik (RME) merujuk pada upaya dan langkah-langkah yang diambil untuk melindungi data pasien dari ancaman, akses tidak sah, kehilangan, atau kerusakan, baik selama penyimpanan, pemrosesan, maupun transmisi. Keamanan data ini bertujuan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi medis elektronik (Suryani, 2024).

b. Komponen Utama Keamanan Data dalam RME:

1) Kerahasiaan (*Confidentiality*)**:**

Memastikan bahwa data pasien hanya dapat diakses oleh individu yang memiliki izin, seperti tenaga medis atau staf administrasi yang berwenang. Ini mencegah akses tidak sah atau bocornya informasi ke pihak ketiga.

2) Integritas *(Integrity*):

Menjaga agar data pasien tetap akurat, lengkap, dan tidak diubah atau dimanipulasi secara tidak sah selama proses penyimpanan dan transmisi. Integritas memastikan bahwa data yang digunakan untuk pengambilan keputusan medis tetap dapat diandalkan.

3) Ketersediaan (*Availability*):

Memastikan bahwa data pasien dapat diakses oleh pengguna yang berwenang kapan pun diperlukan, terutama dalam situasi darurat. Sistem RME harus memiliki mekanisme yang memastikan data selalu tersedia meskipun terjadi gangguan atau serangan *siber*.

4) Otentikasi dan Otorisasi:

Menggunakan mekanisme seperti kata sandi, token, atau biometrik untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses data tertentu, berdasarkan peran dan tanggung jawab mereka dalam organisasi.

5) Audit dan Monitoring:

Mencatat dan memantau semua aktivitas dalam sistem RME untuk mendeteksi dan menanggapi potensi pelanggaran keamanan. Audit trail membantu dalam investigasi dan kepatuhan regulasi.

6) Pencegahan Ancaman dan Serangan:

Implementasi langkah-langkah keamanan teknis seperti firewall, antivirus, enkripsi, dan deteksi intrusi untuk melindungi data dari ancaman eksternal dan internal seperti malware, phishing, atau serangan siber lainnya.

c. Pentingnya Keamanan Data dalam RME:

1) Perlindungan Informasi Sensitif: Mengamankan informasi pribadi dan medis pasien yang sangat sensitif.
2) Meningkatkan Kepercayaan Pasien: Memberikan keyakinan kepada pasien bahwa data mereka dikelola dengan aman.
3) Kepatuhan Hukum dan Etika: Memenuhi persyaratan regulasi dan standar etika dalam pengelolaan data kesehatan.
4) Pencegahan Kerugian Finansial dan Reputasi: Menghindari dampak negatif dari pelanggaran data yang dapat merugikan secara finansial dan merusak reputasi fasilitas kesehatan. (Siahaan, 2024)

Dengan demikian, keamanan data dalam RME adalah fondasi penting dalam memberikan layanan kesehatan yang aman, terpercaya, dan sesuai dengan standar profesional dan hukum.

4. Risiko dan ancaman terhadap keamanan data pasien dalam (RME).

Risiko dan ancaman terhadap keamanan data pasien dalam Rekam Medis Elektronik (RME) dapat berasal dari berbagai sumber, baik internal maupun eksternal. Berikut adalah beberapa risiko dan ancaman yang umum (Kusumo, 2022):

1) Kesalahan Manusia
   a) Kelalaian: Staf yang tidak mengikuti protokol keamanan, seperti meninggalkan perangkat tanpa pengamanan atau membagikan *password*.
   b) Kesalahan Input Data: Memasukkan data yang salah atau tidak lengkap, yang dapat menyebabkan kesalahan dalam diagnosa atau perawatan.
   c) Kehilangan Perangkat: Kehilangan perangkat yang berisi data pasien, seperti laptop atau ponsel, yang tidak diamankan dengan baik.
2) Akses Tidak Sah
   a) Insider Threats: Ancaman dari dalam organisasi, seperti karyawan yang menyalahgunakan akses mereka untuk mencuri atau membocorkan data pasien.
   b) Akses oleh Pihak Ketiga: Pihak ketiga seperti vendor atau kontraktor yang memiliki akses ke sistem RME dapat menjadi risiko jika tidak diawasi dengan baik.
3) Kegagalan Sistem dan Bencana
   a) Kegagalan Hardware/Software: Kerusakan perangkat keras atau perangkat lunak dapat menyebabkan hilangnya data atau gangguan dalam aksesibilitas data.
   b) Bencana Alam: Bencana seperti banjir, gempa bumi, atau kebakaran yang merusak infrastruktur fisik dan menyebabkan hilangnya data jika tidak ada sistem cadangan yang memadai.

4) Pelanggaran Data
   a) *Data Breach*: Pelanggaran data yang disebabkan oleh penyerang yang berhasil mendapatkan akses ke sistem RME dan mencuri informasi pasien.
   b) *Leakage*: Kebocoran data yang disebabkan oleh pengamanan yang lemah atau kesalahan dalam pengelolaan data.

5. Aspek teknis dan non-teknis keamanan data

Dalam pengelolaan Rekam Medis Elektronik (RME), aspek teknis dan non-teknis keamanan data sangat penting untuk melindungi informasi sensitif pasien. Berikut adalah rincian dari kedua aspek tersebut (Ardianto, 2024):

1) Aspek Teknis Keamanan Data
   a) Enkripsi Data:
      – Data in Transit: Menggunakan protokol TLS/SSL untuk melindungi data yang dikirim melalui jaringan.
      – Data at Rest: Menggunakan algoritma enkripsi seperti AES untuk melindungi data yang disimpan.
2) Autentikasi dan Autorisasi:
   a) *Autentikasi Multifaktor* (MFA): Meningkatkan keamanan dengan memerlukan lebih dari satu metode verifikasi.
   b) *Role-Based Access Control* (RBAC): Hanya memberikan akses sesuai dengan peran dan tanggung jawab pengguna.
3) *Firewall* dan Sistem Deteksi/Pencegahan Intrusi (IDS/IPS): Menggunakan *firewall* untuk mencegah akses tidak sah dan IDS/IPS untuk mendeteksi serta merespon aktivitas mencurigakan.
4) Pemantauan dan *Loging*: Menerapkan pemantauan terus-menerus dan *loging* aktivitas untuk mendeteksi dan menganalisis insiden keamanan.
5) *Backup* dan Pemulihan: Membuat cadangan data secara berkala dan memastikan adanya rencana pemulihan bencana untuk mengatasi kehilangan data atau kerusakan sistem.

6) Pembaruan Sistem dan *Patch* Keamanan: Memastikan semua perangkat lunak dan sistem diperbarui dengan patch keamanan terbaru untuk menutup celah keamanan.

6. Teori *CIA Triad*

Teori *CIA Triad* (Confidentiality, Integrity, Availability) adalah kerangka kerja dasar dalam keamanan informasi yang digunakan untuk melindungi data dan sistem dari ancaman (Hidayasari, 2024). Berikut adalah penjelasan masing-masing elemen dalam *CIA Triad*:

1) *Confidentiality* (Kerahasiaan):

Kerahasiaan memastikan bahwa informasi hanya dapat diakses oleh pihak yang memiliki wewenang. Hal ini melibatkan implementasi kontrol akses, autentikasi pengguna, dan enkripsi data untuk melindungi informasi dari akses yang tidak sah.

2) *Integrity* (Integritas):

Integritas menjamin bahwa informasi tetap akurat, utuh, dan tidak berubah tanpa izin. Teknik seperti hashing, checksum, dan kontrol akses berperan dalam mendeteksi dan mencegah perubahan data oleh pihak yang tidak berwenang.

3) *Availability* (Ketersediaan):

Ketersediaan memastikan bahwa sistem dan data dapat diakses oleh pengguna yang berwenang kapan pun diperlukan. Hal ini dicapai melalui infrastruktur yang andal, perlindungan terhadap serangan seperti *denial-of-service* (DoS), dan pemulihan cepat dari bencana atau gangguan sistem.

7. Aspek Parkerian Hexad

Parkerian Hexad adalah model keamanan informasi yang diperkenalkan oleh (Parker , 2002) sebagai perluasan dari model tradisional CIA Triad (*Confidentiality, Integrity, Availability*). Model ini mencakup enam aspek yang saling melengkapi untuk memberikan pendekatan yang lebih komprehensif terhadap keamanan informasi.

a) Merujuk pada upaya untuk memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang. Ini melindungi data dari pengungkapan kepada pihak yang tidak berwenang.

b) *Integrity* (Integritas)

   Menjaga agar data tetap akurat, konsisten, dan tidak diubah tanpa izin. Integritas memastikan bahwa informasi tidak dimodifikasi secara tidak sah, baik selama penyimpanan maupun transmisi.

c) *Availability* (Ketersediaan)

   Memastikan bahwa informasi dan sistem selalu tersedia dan dapat diakses saat dibutuhkan oleh pengguna yang berwenang.

d) *Possession/Control* (Kepemilikan/Kendali Fisik)

   Mengacu pada siapa yang secara fisik memiliki atau mengendalikan informasi. Aspek ini penting karena kehilangan kendali fisik atas data bisa menyebabkan pelanggaran, bahkan jika data tetap terenkripsi.

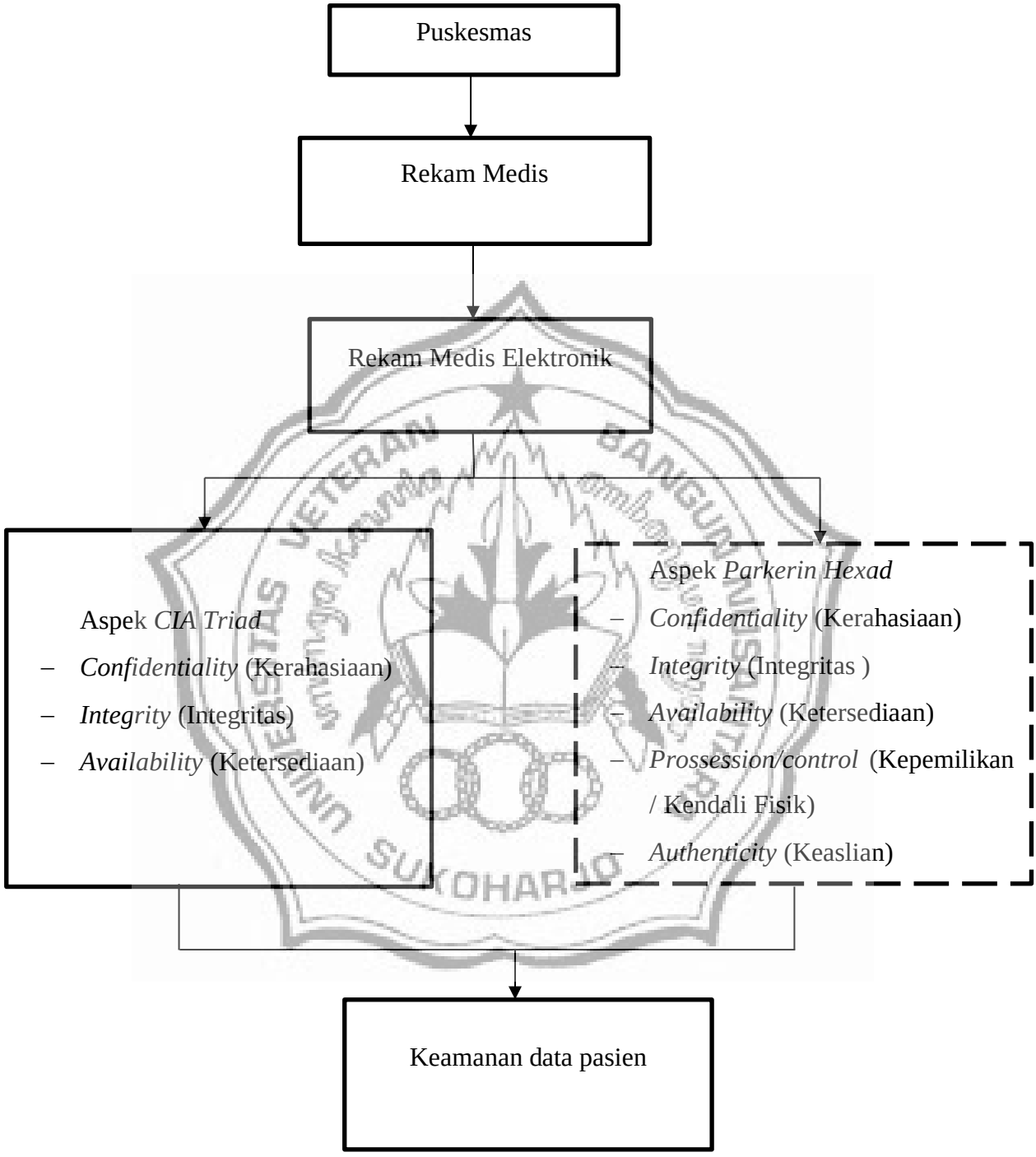
e) *Authenticity* (Keaslian)

   Memastikan bahwa informasi atau sumbernya adalah asli dan dapat dipercaya. Ini berkaitan dengan verifikasi identitas serta keaslian dokumen atau pesan.

f) *Utility* (Kegunaan)

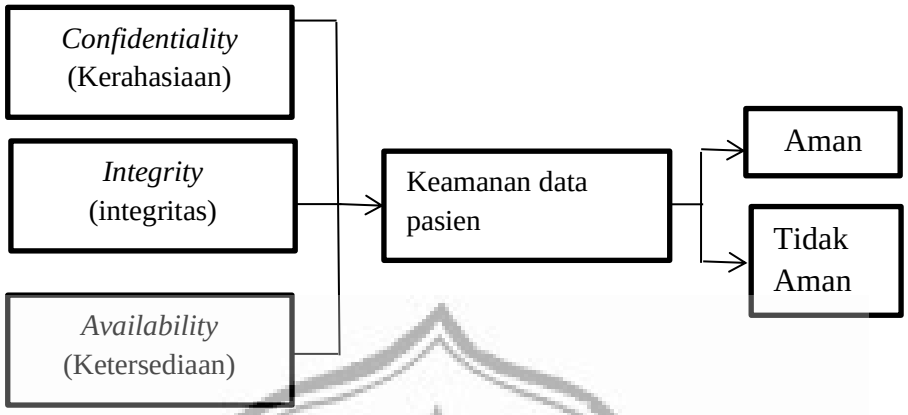
   Mengacu pada sejauh mana data bermanfaat atau dapat digunakan oleh pihak yang berwenang. Data yang sah dan tersedia, tetapi dalam format yang tidak bisa diproses, mungkin tidak berguna.

B. Kerangka Teori



Gambar 2. 1 Kerangka Teori.

C. Kerangka Konsep



Gambar 2. 2 Kerangka Konsep

D. Pertanyaan penelitian

1. Bagaimana penerapan aspek *confidential* pada Rekam Medis Elektronik dipuskesmas Gatak ?
2. Bagaimana penerapan aspek *integrity* pada Rekam Medis Elektronik dipuskesmas Gatak ?
3. Bagaimana penerapan aspek *availability* pada Rekam Medis Elektronik dipuskesmas Gatak ?