BAB I

PENDAHULUAN

A. Latar Belakang

Penyelenggaraan Rekam Medis Elektronik (RME) menurut Permenkes No. 24 Tahun 2022 Tentang Rekam Medis Elektronik menyatakan bahwa Fasilitas Pelayanan Kesehatan (Fasyankes) diwajibkan untuk menerapkan RME dengan batas waktu hingga 31 Desember 2023. Fasyankes yang dimaksudkan tidak hanya rumah sakit melainkan juga Puskesmas. Dalam penyelenggaraan RME di Puskesmas, aspek penting tentang keamanan data medis yang harus dijaga menjadi perhatian utama. Karena RME berisi data medis yang bersifat sensitif. Sistem ini memungkinkan dokter, perawat, dan petugas administrasi mengakses data pasien dengan lebih mudah. Oleh karena itu, penting untuk memastikan keamanan data pasien dari akses yang tidak sah (Gunawan, 2023).

Menurut Helmiawan, *et al*. (2024), tiga prinsip dalam keamanan data mencakup *Confidentiality* (Kerahasiaan), *Integrity* (Integritas), dan *Availability* (Ketersediaan). Standar internasional *ISO/IEC 27001* juga menekankan prinsip serupa dalam penerapan keamanan data. Penelitian terdahulu memberikan gambaran nyata tentang tantangan dalam penerapan keamanan data RME di berbagai fasilitas kesehatan. Penelitian oleh Tiorentap

dan Hosizah (2020) menyatakan bahwa sistem keamanan yang ada pada RME masih lemah, yaitu masih ada praktik berbagi *user-ID* dan *password*, sehingga sulit melacak siapa yang mengakses data jika terjadi kesalahan. Sementara itu, penelitiaan oleh Ardianto dan Nurjanah (2024) menunjukkan kelemahan, seperti *username* dan *password* yang jarang diganti serta waktu *logout* otomatis yang terlalu lama sehingga dapat meningkatkan risiko akses yang tidak sah dan memungkinkan penyalahgunaan data pasien.

Hasil survei yang telah dilakukan di UPT Puskesmas Kebakkramat I, ditemukan bahwa keamanan data pasien pada SIMPUS belum terdapat sistem *Automatic Log Off* pada sistem keamanan data. *Automatic Log Off* merupakan mekanisme keamanan yang secara otomatis mengakhiri sesi pengguna setelah periode tidak aktif tertentu, sehingga dapat mencegah akses tidak sah terhadap data sensitif. Ketiadaan ALO ini meningkatkan potensi risiko keamanan yang dapat mengakibatkan kebocoran informasi medis.

Berdasarkan hasil survei yang telah dilakukan di atas, maka penulis tertarik melakukan penelitian dengan judul "Penerapan Keamanan Data Rekam Medis Elektronik Pada Sistem Informasi Manajemen Puskesmas (SIMPUS) di UPT Puskesmas Kebakkramat I".

B. Perumusan Masalah

Rumusan masalah yang diambil berdasarkan pada latar belakang di atas adalah bagaimana penerapan keamanan data rekam medis elektroik pada SIMPUS di UPT Puskesmas Kebakkramat I?

C. Tujuan

1. Tujuan Umum

   Untuk menganalisis penerapan keamanan data rekam medis elektronik pada SIMPUS di UPT Puskesmas Kebakkramat I.

2. Tujuan Khusus

   a. Menganalisis penerapan keamanan data rekam medis elektronik pada SIMPUS di UPT Puskesmas Kebakkramat I pada aspek *confidentiality*.

   b. Menganalisis penerapan keamanan data rekam medis elektronik pada SIMPUS di UPT Puskesmas Kebakkramat I pada aspek *integrity.*

   c. Menganalisis penerapan keamanan data rekam medis elektronik pada SIMPUS di UPT Puskesmas Kebakkramat I pada aspek *availability*.

D. Manfaat

1. Bagi Puskesmas

   Sebagai bahan pertimbangan terkait keamanan data pada Sistem Informasi Manajemen Puskesmas (SIMPUS).

2. Bagi Instansi Pendidikan

   Sebagai *literature* dan referensi pembelajaran tentang aspek keamanan data rekam medis elektronik pada SIMPUS.

3. Bagi Mahasiswa

   Sebagai acuan pembelajaran mengenai keamanan data rekam medis elektronik pada SIMPUS.

BAB II

TINJAUAN PUSTAKA

A. Teori Yang Relevan

1. Puskesmas

   a. Pengertian Puskesmas

      Puskesmas menurut Permenkes No. 19 Tahun 2024 Tentang Penyelenggaraan Pusat Kesehatan Masyarakat adalah Fasilitas Pelayanan Kesehatan tingkat pertama yang menyelenggarakan dan mengoordinasikan pelayanan kesehatan promotif, preventif, kuratif, rehabilitatif, dan/atau paliatif di wilayah kerjanya.

   b. Prinsip penyelenggaraan Puskesmas berdasarkan Permenkes No. 19 Tahun 2024 Tentang Penyelenggaraan Pusat Kesehatan Masyarakat meliputi:

      1) Paradigma Sehat
      2) Pertanggungjawaban Wilayah
      3) Kemandirian Masyarakat
      4) Ketersediaan Akses Pelayanan Kesehatan
      5) Teknologi Tepat Guna
      6) Keterpaduan dan Kesinambungan

2. Sistem Informasi Manajemen Puskesmas (SIMPUS)

   a. Pengertian SIMPUS

      Menurut Permenkes No 19 Tahun 2024 Sistem Informasi Puskesmas adalah suatu tatanan yang menyediakan informasi untuk

membantu proses pengambilan keputusan dalam melaksanakan manajemen Puskesmas dalam mencapai sasaran kegiatannya.

b. Tujuan SIMPUS

Berdasarkan Permenkes No 31 Tahun 2019 Sistem Informasi Puskesmas bertujuan untuk:

1) Mewujudkan penyelenggaraan Sistem Informasi Puskesmas yang terintegrasi;
2) Menjamin ketersediaan data dan informasi yang berkualitas, berkesinambungan, dan mudah diakses; dan
3) Meningkatkan kualitas pembangunan kesehatan di wilayah kerjanya melalui penguatan manajemen Puskesmas.

c. Keamanan dan Kerahasiaan SIMPUS

Menurut Permenkes No 31 Tahun 2019 Sistem Informasi Puskesmas Pasal 27 bahwa setiap pengelola dan pemangku kepentingan dalam penyelenggaraan Sistem Informasi Puskesmas harus menjamin keamanan dan kerahasiaan informasi sesuai dengan ketentuan peraturan perundang-undangan.

3. Rekam Medis

a. Pengertian Rekam Medis

Menurut permenkes nomor 24 tahun 2022 tentang rekam medis adalah berkas berisi catatan dan dokumen tentang pasien yang berisi identitas pasien, pemeriksaan, pengobatan, tindakan, dan pelayanan lain yang telah diberikan kepada pasien. Setiap fasilitas pelayanan

kesehatan wajib menyelenggarakan rekam medis elektronik. Penyelenggaraan rekam medis elektronik paling sedikit meliputi:

1) Registrasi pasien
2) Pendistribusian data rekam medis
3) Pengisian informasi klinis
4) Pengolahan informasi rekam medis elektronik
5) Penginputan data untuk klaim pembiayaan
6) Penyimpanan rekam medis elektronik
7) Penjaminan mutu rekam medis elektronik
8) Transfer isi rekam medis elektronik

Rekam medis rawat jalan sekurang-kurangnya berisi identitas pasien, pemeriksaan fisik, diagnosis, tindakan atau pengobatan, serta pelayanan lain yang telah diberikan kepada pasien

b. Isi Rekam Medis

Isi Rekam Medis Pada Peraturan Menteri Kesehatan No. 24 Pasal 26 menjelaskan tentang isi rekam medis yaitu;

1) Isi Rekam Medis milik Pasien.
2) Isi Rekam Medis disampaikan kepada Pasien.
3) Selain kepada Pasien, Rekam Medis dapat disampaikan kepada keluarga terdekat atau pihak lain.
4) Penyampaian Rekam Medis kepada keluarga terdekat dilakukan dalam hal: Pasien di bawah umur 18 (delapan belas) tahun; dan/atau Pasien dalam keadaan darurat.

5) Penyampaian Rekam Medis kepada pihak lain dilakukan setelah mendapat persetujuan dari Pasien.
6) Isi Rekam Medis paling sedikit terdiri atas:
    a) Identitas Pasien
    b) Hasil pemeriksaan fisik dan penunjang
    c) Diagnosis, pengobatan, dan rencana tindak lanjut pelayanan kesehatan
    d) Nama dan tanda tangan Tenaga Kesehatan pemberi pelayanan kesehatan.

c. Tujuan Rekam Medis

Menurut Permenkes No. 24 Tahun 2022 Pasal 2, pengaturan Rekam Medis bertujuan untuk:

1) Meningkatkan mutu pelayanan kesehatan;
2) Memberikan kepastian hukum dalam penyelenggaraan dan pengelolaan Rekam Medis;
3) Menjamin keamanan, kerahasiaan, keutuhan, dan ketersediaan data Rekam Medis; dan
4) Mewujudkan penyelenggaraan dan pengelolaan Rekam Medis yang berbasis digital dan terintegrasi

4. Keamanan Data dan Informasi

a. Menurut Permekes No. 24 Tahun 2022 Pasal 29 tentang rekam medis menjelaskan bahwa keamanan data dan informasi memiliki tiga prinsip, yaitu:

1) 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 penggunaan dan penyebarannya.
2) Integritas (*Integrity*) 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.
3) Ketersediaan (*Availability*) 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.

b. Rahadjo (2021) menyatakan bahwa keamanan data memiliki aspek, yaitu:
1) Kerahasiaan (*Confidentiality)* adalah hanya orang atau sistem yang berwenang yang dapat mengakses data yang dilindungi. C*onfidentiality* ini bisa berarti sama dengan privasi. Ini juga merupakan serangkaian langkah-langkah yang perlu dilakukan untuk mencegah terekspos nya informasi sensitif dari jangkauan tangan orang-orang yang tidak berwenang. Tak hanya itu, juga harus dipastikan bahwa orang yang tepat sudah benar-benar mendapatkan data yang dibutuhkan. Misalnya, siapa yang

menentukan orang atau sistem mana yang berwenang untuk mengakses sistem saat ini. Perlindungan terhadap aspek *confidentiality* dapat dilakukan dengan menggunakan kriptografi dan membatasi akses (segmentasi jaringan).

2) Integritas (*Integrity),* ini berarti menjaga konsistensi, akurasi, dan kepercayaan terhadap data untuk setiap waktu hingga seterusnya. Data tidak boleh diubah pada saat transit. Kemudian juga langkah-langkah tertentu perlu dilakukan untuk memastikan bahwa data tidak bisa diubah-ubah oleh orang yang tidak punya kepentingan sejalan (misalnya, para peretas yang ingin melakukan manipulasi data). Langkah-langkah tersebut juga termasuk izin dalam mengakses *file* dan batasan kontrol bagi akses pengguna. Kontrol ini bisa dipakai untuk mencegah perubahan yang keliru atau penghapusan tidak disengaja dari pengguna resmi yang bisa juga menjadi masalah. Integritas dapat ditegakkan dengan cara yang sama seperti kerahasiaan: dengan kontrol yang ketat terhadap siapa atau apa yang dapat mengakses sumber daya mana dengan cara apa.
3) Ketersediaan *(Availability)* ketersediaan berlaku untuk data dan layanan (yaitu, untuk informasi dan pemrosesan informasi). Misalnya, objek atau layanan dianggap tersedia jika layanan selesai dalam jangka waktu yang dapat diterima. Hal ini membuat kemajuan yang jelas, dan jika dalam mode tunggu, memiliki

waktu tunggu yang terbatas. Namun, banyak dari kita mengalami kelebihan beban: akses semakin lambat; komputer merespons tetapi tidak dengan cara yang kami anggap normal atau dapat diterima.

c. Menurut Helmiawan, et al (2024), keamanan informasi terdiri dari tiga pinsip utama, yaitu:

1) *Confidentiality* (Kerahasiaan) adalah prinsip yang berfokus pada memastikan bahwa informasi hanya dapat diakses oleh pihak yang memiliki otoritas atau izin yang sah. Untuk menjaga kerahasiaan, teknik seperti enkripsi data, kontrol akses berbasis peran *(Role-Based Access Control)*, dan penggunaan kata sandi atau otentikasi dua faktor (*Two-Factor Authentication*) sering kali diterapkan. Tujuannya adalah mencegah pihak yang tidak berwenang melihat atau menggunakan informasi sensitif, sehingga kerahasiaan informasi tetap terjaga.

2) *Integrity* (Integritas) menekankan pada pentingnya menjaga keutuhan dan konsistensi data sepanjang siklus hidupnya. Integritas berarti bahwa data tidak boleh diubah atau dimodifikasi oleh pihak yang tidak berwenang. Untuk memastikan integritas data, berbagai metode digunakan, seperti *checksum*, *digital signatures*, penggunaan *hashing algorithms*, dan *audit trial* dan *logging*. Dengan menjaga integritas data, organisasi dapat yakin

bahwa informasi yang mereka gunakan dapat dipercaya dan tidak dimanipulasi oleh pihak yang tidak bertanggung jawab.

3) *Availability* (Ketersediaan) mengacu pada kemampuan sistem untuk menyediakan akses ke informasi bagi pengguna yang sah kapan pun diperlukan. Prinsip ini menekankan bahwa informasi harus selalu dapat diakses oleh pengguna yang berwenang tanpa adanya gangguan atau hambatan yang tidak diinginkan. Untuk menjaga ketersediaan, tindakan seperti pemeliharaan sistem secara rutin, penggunaan *backup* dan *failover systems*, serta perlindungan terhadap serangan *denial-of-service* (DoS) diterapkan.

5. Standar Jarak *Back-Up* Data

a. Pacheco (2020) menyatakan bahwa dalam perencanaan pemulihan bencana (*disaster recovery*), penting untuk memastikan bahwa pusat data utama dan lokasi cadangan berada pada jarak yang cukup jauh untuk menghindari dampak dari bencana yang sama. Meskipun tidak ada aturan baku, Pacheco merekomendasikan jarak minimal 100 mil (sekitar 160 kilometer) antara kedua lokasi tersebut. Hal ini bertujuan agar jika terjadi bencana alam atau gangguan besar lainnya, kedua fasilitas tidak terdampak secara bersamaan, sehingga kontinuitas operasional tetap terjaga.

b. Menurut Aktaş (2020) dalam menentukan jarak ideal antara pusat data utama dan situs pemulihan bencana, perlu mempertimbangkan mitigasi risiko terhadap bencana lokal (seperti gempa, banjir) serta

kebutuhan untuk pemulihan cepat. Menurut Aktaş, jarak yang direkomendasikan adalah untuk mengurangi sebagian besar risiko, menempatkan lokasi pemulihan bencana di suatu tempat antara 30 mil (50 kilometer) dan 100 mil (160 kilometer) dari lokasi utama. Namun dengan melakukan penilaian risiko terlebih dahulu. Jarak yang terlalu dekat meningkatkan risiko terkena dampak bencana yang sama, sedangkan jarak yang terlalu jauh dapat memperlambat proses pemulihan data. Selain jarak, faktor kecepatan koneksi dan target waktu pemulihan (*Recovery Time Objective* - RTO) juga harus diperhatikan.

B. Penelitian Yang Relevan

1. Penelitian oleh Widiyanti, Hastuti dan Kusumawati (2024) dengan judul "Tinjauan Keamanan Data Rekam Medis Elektronik Pada Aplikasi SIMPUS Berdasarkan Aspek C*onfidentiality, Integrity dan Availability* Di Puskesmas Tasikmadu Karanganyar". Penelitian ini menggunakan metode deskriptif dengan pendekatan kualitatif. Data dikumpulkan melalui wawancara dan observasi dengan pedoman wawancara tidak terstruktur. Hasil penelitian menunjukkan bahwa keamanan data pada aspek *confidentiality* sudah terjaga karena pengguna harus *login* dengan *username* dan *password*. Namun, SIMPUS belum memiliki fitur *Automatic Log Off*. Pada aspek *integrity*, data aman karena hanya bisa diedit oleh pengguna terkait, sementara penghapusan hanya bisa

dilakukan oleh pihak berwenang. Dalam aspek *availability*, data selalu tersedia saat dibutuhkan dan dapat diakses dari mana saja dengan hak akses. Namun, proses *back-up* masih dilakukan secara manual setiap hari atau secara berkala dan belum otomatis *back-up.*

2. Penelitian oleh Rahma dan Suryani (2024) dengan judul "Analisis Penggantian *Password User Id* dalam Sistem Rekam Medis Elektronik Guna Menjaga Keamanan Data Rekam Medis di Rumah Sakit Hermina Arcamanik". Jenis penelitian yang digunakan adalah kualitatif deskriptif. Cara pengumpulan data adalah wawancara dan observasi. Penelitian ini menunjukkan bahwa sistem keamanan dilakukan dengan penggunaan *password user id*. Akan tetapi, penggunaan *password user id* oleh petugas kurang efisien dilihat dari banyaknya petugas dalam satu *shift* yang mengerjakan satu pekerjaan secara bergantian sehingga petugas sering lupa *log-out id* pengguna mereka. Hal ini dapat menyebabkan risiko penyalahgunaan *user id.*
3. Penelitian oleh Lissa, Maiyestati dan Zarfinal (2023) dengan judul "Implementasi Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 Tentang Rekam Medis di RSUP M. Djamil Padang (Keamanan dan Perlindungan Data Rekam Medis Elektronik)". Jenis penelitian yang digunakan adalah kualitatif yang bersifat deskriptif. Sumber data yang digunkan yaitu data primer dari hasil wawancara dan studi dokumen. Penelitian ini menunjukkan bahwa pada aspek *confidentiality*, pengguna (*user*) saling membagikan *password* kepada petugas lain atau komputer

dibiarkan dalam keadaan terbuka. Pada aspek *integrity* keakuratan data belum sepenuhnya terlaksana karena kurangnya kepedulian DPJP dalam menginput data dan belum menyertakan tandatangan elektronik.

4. Penelitian oleh Pradita, Kusumo, dan Rahmawati (2022) dengan judul "Pentingnya Aspek Keamanan Informasi Data Pasien Pada Penerapan RME di Puskesmas". Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan studi kasus di beberapa Puskesmas di wilayah Jawa Tengah. Data dikumpulkan melalui wawancara mendalam dengan kepala Puskesmas, tenaga kesehatan, dan petugas IT, serta observasi langsung pada sistem yang digunakan. Penelitian ini menunjukkan bahwa e-Puskesmas belum sepenuhnya aman karena data bisa diakses oleh pihak yang tidak berwenang. Selain itu, pencatatan rekam medis elektronik perlu diperbaiki agar data lebih mudah diubah dan tersedia untuk klaim BPJS. Tim PKM merekomendasikan penggunaan *username* dan *password* individu, fitur *log out* otomatis, pemblokiran akses jaringan, enkripsi data, integrasi dengan aplikasi BPJS, dan sistem *back-up* untuk melindungi data pasien.
5. Penelitian oleh Nugraheni dan Nurhayati (2018) dengan judul "Aspek Hukum Rekam Medis Elektronik di RSUD Dr. Moewardi". Jenis penelitian yang digunakan adalah deskriptif kualitatif. dengan pendekatan yuridis normatif. Data diperoleh melalui studi dokumen dan wawancara mendalam dengan staf rumah sakit dan ahli hukum kesehatan. Penelitian ini menunjukkan pada aspek *confidentiality* dijaga dengan

penggunaan *username* dan *password* untuk setiap pengguna. Namun, dalam aspek *integrity* penghapusan data belum tersedia. Sementara itu, aspek *Avalilability* sudah terpenuhi, tetapi belum maksimal karena masih diperlukan dokumen rekam medis kertas, terutama untuk pasien rawat jalan yang dirujuk untuk rawat inap dan pemeriksaan lebih lanjut.

BAB III

METODE PENELITIAN

A. Rancangan Penelitian

Penelitian ini menggunakan jenis penelitian deskriptif dengan pendekatan kualitatif untuk menggambarkan keamanan data rekam medis elektronik pada SIMPUS berdasarkan aspek *confidentiality, integrity* dan *availability* di UPT Puskesmas Kebakkramat I.

B. Lokasi dan Waktu Penelitian

1. Lokasi Penelitian

   Penelitian ini dilakukan pada bagian pendaftaran rawat jalan di UPT Puskesmas Kebakkramat I.

2. Waktu Penelitian

   Kegiatan penelitian ini dilakukan pada Februari-April 2025.

C. Subjek dan Objek

1. Subjek Penelitian

   Subjek dari penelitian ini yaitu pengguna SIMPUS, meliputi Kepala Puskesmas dan dua Staf Pendaftaran Rawat Jalan.

2. Objek Penelitian

   Pada objek penelitian ini yaitu Sistem Informasi Manajemen (SIMPUS) bagian pendaftaran rawat jalan.

D. Definisi Konsep

Tabel 3.1
Definisi Konsep

No.	Konsep	Definisi Konsep
1.	*Confidentiality*	Penjagaan informasi dari pihak-pihak yang tidak memiliki hak akses untuk mengakses informasi tersebut sehingga data dan informasi yang ada di SIMPUS dapat tejamin keamanannya.
2.	*Integrity*	Menjamin data yang telah dientry tidak diubah oleh pihak manapun dengan melihat *audit trail* (telusur data).
3.	*Availability*	Menjamin data dan informasi yang ada dalam SIMPUS dapat diakses dan digunakan oleh orang yang telah memiliki hak akses saat dibutuhkan.

E. Instrumen dan Cara Pengumpulan Data

1. Instrumen Penelitian

   a. Pedoman Observasi

      Pedoman observasi yang digunakan pada penelitian ini adalah daftar pengamatan yang dibutuhkan dalam penelitian tentang perlindungan keamanan data pada Sistem Informasi Manajemen (SIMPUS) berdasarkan aspek *confidentiality, integrity* dan *availability* di UPT Puskesmas Kebakkramat I.

   b. Pedoman Wawancara

      Pada penelitian ini, peneliti telah menyiapkan instrumen penelitian berupa daftar pertanyaan mengenai keamanan data pada Sistem Informasi Manajemen (SIMPUS).

2. Cara Pengumpulan Data

   a. Observasi

      Melakukan pengamatan terhadap terhadap penggunaan Sistem Informasi Manajemen (SIMPUS).

   b. Wawancara

      Pada penelitian ini menggunakan wawancara terstruktur dengan proses tanya jawab kepada responden yaitu Kepala Puskesmas dan Staff Pendaftaran Rawat Jalan, guna memperoleh informasi mengenai keamanan SIMPUS di UPT Puskesmas Kebakkramat I.

F. Keabsahan Data

Keabsahan data dalam penelitian ini menggunakan Triangulasi Sumber dan Triangulasi Metode.

1. Triangulasi Sumber

   Membandingkan informasi yang diperoleh dari dua staf pendaftaran rawat jalan dengan informasi dari Kepala Puskesmas untuk memastikan keakuratan dan konsistensi terkait hasil wawancara tentang keamanan data pada SIMPUS.

2. Triangulasi Metode

   Membandingkan hasil pengumpulan data melalui wawancara dan observasi terhadap sistem keamanan data rekam medis yang digunakan pada SIMPUS.

G. Teknik Pengolahan dan Analisis Data

1. Teknik Pengolahan Data

   Data yang terkumpul akan dilakukan pengolahan dengan tahap:

   a. Reduksi Data

      Membuat ringkasan, memilih hal-hal yang pokok, dan memusatkan perhatian pada yang penting mengenai keamanan data rekam medis elektronik pada SIMPUS di UPT Puskesmas Kebakkramat I.

   b. Penyajian Data

      Menyajikan hasil penelitian dalam bentuk uraian kalimat sehingga pembaca dapat dengan mudah memahami tentang keamanan data rekam medis elektronik pada SIMPUS di UPT Puskesmas Kebakkramat I.

   c. Penarikan Kesimpulan

      Penarikan kesimpulan disesuaikan dengan tujuan khusus yang meliputi keamanan data rekam medis elektronik pada SIMPUS di UPT Puskesmas Kebakkramat I pada aspek *confidentiality, integrity*, dan *availability*.

2. Analisis Data

   Analisis data yang digunakan penelitian ini adalah deskriptif yang merupakan menganalisis dan menjelaskan hasil penelitian sesuai dengan keadaan sebenar-benarnya mengenai keamanan SIMPUS berdasarkan

aspek *confidentiality, integrity*, dan *availability* di UPT Puskesmas Kebakkramat I.

H. Jadwal Penelitian

Tabel 3.2
Jadwal Penyusunan Karya Tulis Ilmiah Tahun 2025

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																				