BAB 1 PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi telah mendorong digitalisasi dalam pelayanan kesehatan, termasuk dalam pengelolaan informasi medis pasien. Penerapan rekam medis elektronik memberikan kemudahan dalam penyimpanan, pengolahan, dan akses terhadap informasi kesehatan sehingga informasi pasien dapat digunakan secara lebih efektif dalam mendukung pelayanan kesehatan. Perkembangan rekam medis elektronik juga telah menjadi bagian dari transformasi sistem informasi kesehatan di berbagai negara dan fasilitas pelayanan kesehatan (Häyrinen et al., 2008). Di Indonesia, penerapan rekam medis elektronik juga terus berkembang dan menuntut fasilitas pelayanan kesehatan untuk memperhatikan aspek keamanan serta kerahasiaan informasi pasien (Pramesti et al., 2024).

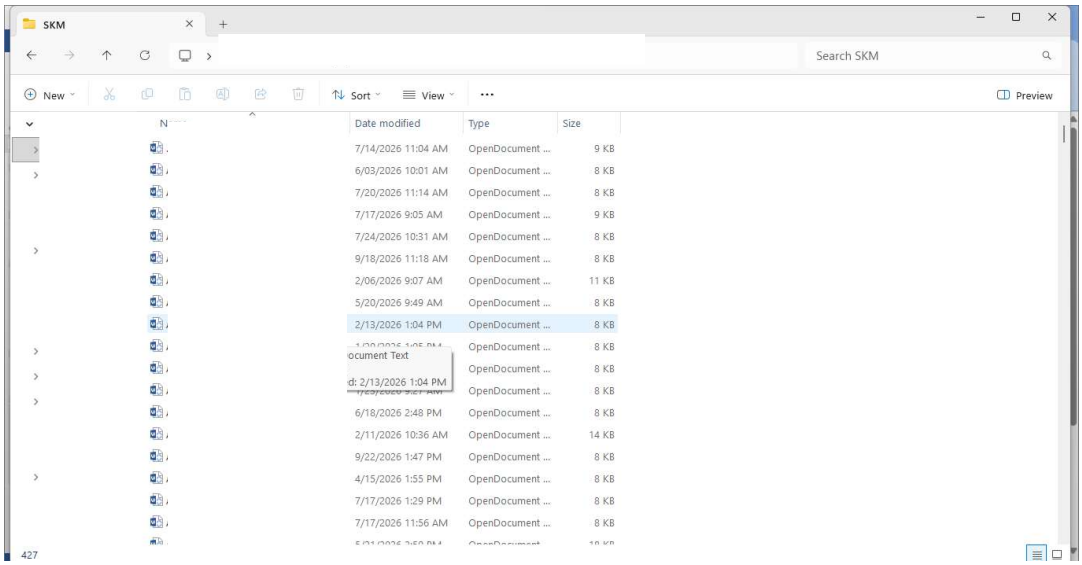
Digitalisasi informasi kesehatan di sisi lain menimbulkan tantangan dalam aspek keamanan karena informasi yang tersimpan secara elektronik dapat menghadapi risiko akses atau penggunaan oleh pihak yang tidak berwenang. Data medis pasien memiliki sifat sensitif karena dapat memuat identitas pasien, riwayat pelayanan, diagnosis, hasil pemeriksaan, serta informasi kesehatan lainnya yang berkaitan dengan kondisi pasien. Hasil tinjauan sistematis mengenai keamanan dan kerahasiaan data medis menunjukkan bahwa perlindungan terhadap informasi pasien menjadi aspek penting dalam penerapan rekam medis elektronik untuk mencegah terjadinya kebocoran dan akses yang tidak sah (Pramesti et al., 2024). Penelitian lain mengenai keamanan data rekam medis elektronik juga menunjukkan bahwa aspek privasi, integritas, autentikasi, dan kontrol akses perlu diperhatikan dalam pengelolaan data pasien secara elektronik (Ikawati et al., 2025).

Salah satu pendekatan teknis yang dapat digunakan untuk memberikan perlindungan tambahan terhadap informasi sensitif adalah kriptografi melalui proses enkripsi. Enkripsi merupakan proses mengubah data asli (*plaintext*) menjadi bentuk yang tidak dapat dibaca secara langsung (*ciphertext*) sehingga informasi tersebut memerlukan proses dekripsi dan kunci yang sesuai untuk dapat dikembalikan ke bentuk aslinya. Salah satu algoritma kriptografi yang dapat digunakan adalah *Advanced Encryption Standard* (AES), yaitu algoritma kriptografi simetris yang banyak digunakan untuk mengamankan data elektronik. AES menggunakan kunci dengan panjang 128, 192, atau 256 bit dan dapat digunakan dalam proses enkripsi maupun dekripsi data. Penerapan teknik kriptografi pada rekam medis elektronik juga telah dikaji sebagai salah satu upaya untuk menjaga kerahasiaan dan keamanan informasi pasien (Febriyana & Ichwani, 2024).

Berdasarkan hasil observasi selama pelaksanaan Praktik Kerja Lapang (PKL) pada bagian Surat Keterangan Medis (SKM) di Rumah Sakit Bethesda Yogyakarta, ditemukan kondisi yang berkaitan dengan keamanan file yang memuat informasi pasien. Bagian SKM melayani pembuatan dan pengelolaan berbagai dokumen pasien, seperti surat keterangan kematian, surat keterangan kelahiran, surat keterangan medis, surat izin, dan surat rujukan. Dokumen-dokumen tersebut dapat memuat identitas serta informasi kesehatan pasien sehingga kerahasiaannya perlu dijaga selama proses pembuatan, penyimpanan, maupun pendistribusian kepada pasien. Kondisi tersebut sejalan dengan penelitian mengenai keamanan rekam medis elektronik yang menempatkan kerahasiaan dan privasi informasi pasien sebagai aspek penting dalam pengelolaan informasi kesehatan (Ikawati et al., 2025).

Selain itu, berdasarkan hasil observasi, terdapat permintaan pasien untuk menerima dokumen melalui aplikasi *WhatsApp*. Pengiriman dokumen yang memuat informasi pasien melalui media elektronik menyebabkan file dapat tersimpan pada perangkat penerima dan berpotensi diteruskan kepada pihak lain. Oleh karena itu,

diperlukan perlindungan tambahan terhadap file sebelum didistribusikan kepada pasien. Salah satu alternatif yang dapat digunakan adalah mengenkripsi file terlebih dahulu sehingga isi dokumen tidak dapat langsung dibaca tanpa adanya password atau kunci yang sesuai. Pendekatan tersebut memiliki keterkaitan dengan penelitian mengenai penerapan kriptografi untuk pengamanan data rekam medis, yang menunjukkan bahwa enkripsi dapat digunakan untuk memberikan perlindungan terhadap informasi kesehatan pada saat data disimpan maupun dipertukarkan secara elektronik (Tamin & Hendrik, 2025). Adapun kondisi penyimpanan dokumen pada bagian SKM dapat dilihat pada gambar berikut.



Gambar 1.1 Tempat Penyimpanan File SKM di RS Bethesda Yogyakarta

Selain permasalahan pada proses pendistribusian file, berdasarkan hasil observasi pada perangkat komputer yang digunakan dalam pelayanan di bagian SKM, ditemukan komputer tanpa adanya autentikasi berupa kata sandi pada perangkat. Kondisi tersebut dapat meningkatkan potensi akses terhadap file yang tersimpan pada perangkat apabila komputer ditinggalkan dalam keadaan aktif atau digunakan oleh pihak yang tidak memiliki kewenangan. Penelitian mengenai keamanan data rekam medis juga menunjukkan bahwa mekanisme autentikasi dan pengendalian akses

merupakan bagian penting dalam menjaga keamanan informasi pasien (Ikawati et al., 2025; Mariani, 2025). Meskipun sistem informasi yang digunakan dapat memiliki mekanisme pengamanan dan pengaturan hak akses tersendiri, perlindungan pada tingkat perangkat dan file tetap dapat digunakan sebagai lapisan keamanan tambahan untuk mengurangi risiko akses tidak sah.

Berdasarkan kondisi tersebut, diperlukan perlindungan terhadap file dokumen pasien yang tidak hanya bergantung pada keamanan perangkat atau sistem informasi, tetapi juga pada keamanan file itu sendiri. Salah satu alternatif yang dapat diterapkan adalah enkripsi menggunakan algoritma AES sehingga file yang akan disimpan atau didistribusikan terlebih dahulu diubah menjadi bentuk terenkripsi. Dalam rancangan prototipe, petugas dapat memilih file dokumen, melakukan proses enkripsi menggunakan algoritma AES dengan password tertentu, kemudian menghasilkan file terenkripsi yang dapat dikirimkan kepada pasien melalui media elektronik. Pasien selanjutnya dapat menggunakan password yang sesuai untuk melakukan proses dekripsi sehingga file dapat dikembalikan ke bentuk aslinya. Konsep pengamanan file menggunakan AES tersebut didukung oleh penelitian Tamin dan Hendrik (2025) yang menerapkan AES-128 untuk mengamankan file rekam medis pasien melalui proses enkripsi dan dekripsi.

Berdasarkan permasalahan yang ditemukan selama pelaksanaan PKL, diperlukan suatu prototipe sistem keamanan file surat menyurat pasien menggunakan algoritma AES yang dapat memberikan gambaran mengenai proses enkripsi dan dekripsi dokumen yang mengandung informasi pasien. Prototipe tersebut dirancang untuk memungkinkan petugas mengenkripsi file sebelum disimpan atau dikirimkan kepada pasien, sedangkan proses dekripsi dilakukan menggunakan password yang sesuai agar file dapat kembali diakses dalam bentuk aslinya. Dengan adanya prototipe tersebut, diharapkan dapat memberikan alternatif perlindungan tambahan terhadap kerahasiaan file surat menyurat pasien serta menjadi gambaran awal dalam

pengembangan mekanisme keamanan dokumen medis yang lebih komprehensif di fasilitas pelayanan kesehatan.

1.2 Tujuan dan Manfaat

1.2.1 Tujuan Umum Magang/PKL

Secara umum, penelitian ini bertujuan untuk mengembangkan prototipe sistem keamanan file surat menyurat pasien yang mampu meningkatkan perlindungan kerahasiaan, integritas, dan keamanan data pasien di Rumah Sakit Bethesda Yogyakarta melalui penerapan algoritma Advanced Encryption Standard (AES).

1.2.2 Tujuan Khusus Magang/PKL

Adapun tujuan khusus magang adalah sebagai berikut.

a. Mengidentifikasi kondisi keamanan dan kerahasiaan file SKM (Surat Keterangan Medis) Pasien di Rumah Sakit Bethesda Yogyakarta.
b. Mengidentifikasi kebutuhan keamanan file SKM (Surat Keterangan Medis) pasien dalam proses penyimpanan dan pengiriman dokumen secara elektronik.
c. Merancang prototipe sistem keamanan file surat menyurat pasien menggunakan algoritma *Advanced Encryption Standard* (AES).
d. Mengimplementasikan algoritma AES pada prototipe sistem untuk melakukan proses enkripsi dan dekripsi file surat menyurat pasien.

1.2.3 Manfaat Magang/PKL

Berikut adalah manfaat magang ini bagi beberapa pihak yang terkait, diantaranya:

a. Bagi RS Bethesda Yogyakarta

   Sebagai bahan masukan dan rekomendasi bagi pihak rumah sakit, khususnya bagian teknologi informasi, dalam meningkatkan keamanan dan

kerahasiaan file surat menyurat pasien melalui penerapan enkripsi menggunakan algoritma *Advanced Encryption Standard* (AES), terutama pada proses penyimpanan dan pengiriman dokumen secara elektronik.

b. Bagi Politeknik Negeri Jember

Sebagai salah satu bahan referensi dan dokumentasi terkait penerapan algoritma *Advanced Encryption Standard* (AES) dalam pengamanan file surat menyurat pasien yang dapat bermanfaat bagi kegiatan pembelajaran dan pengembangan pengetahuan di Politeknik Negeri Jember, khususnya pada Program Studi Manajemen Informasi Kesehatan.

c. Bagi Mahasiswa

Laporan ini diharapkan dapat menambah pengetahuan dan keterampilan mahasiswa dalam menerapkan konsep keamanan informasi, khususnya penggunaan algoritma *Advanced Encryption Standard* (AES) untuk mengamankan file yang mengandung informasi pasien, serta menjadi wadah untuk mengaplikasikan teori yang telah diperoleh selama perkuliahan ke dalam kondisi yang ditemukan di lapangan.

1.3 Lokasi dan Waktu

1.3.1 Lokasi Magang/PKL

Kegiatan Magang Manajemen Klaim dan Unit Kerja Rekam Medis serta Analisis Perancangan Sistem Informasi Kesehatan dilakukan di Rumah Sakit Bethesda Yogyakarta yang berlokasi di Jalan Jenderal Sudirman No. 70, Kotabaru, Kec.Gondokusuman, Kota Yogyakarta – Daerah Istimewa Yogyakarta, 55224.

1.3.2 Waktu Magang/PKL

Waktu kegiatan Magang Manajemen Klaim dan Unit Kerja Rekam Medis serta Analisis Perancangan Sistem Informasi Kesehatan ini dilakukan pada:

a. Tanggal : 03 Agustus 2026 – 24 Oktober 2026

b. Hari Kerja : Senin – Sabtu
c. Jam Kerja : 07.00 – 14.00 WIB

1.4 Metode Pelaksanaan

1.4.1 Jenis Penelitian

Jenis penelitian yang digunakan dalam penelitian ini adalah informasi teknologi yang bertujuan untuk mengidentifikasi dan menggambarkan kondisi keamanan serta kerahasiaan file surat menyurat pasien pada bagian Surat Keterangan Medis (SKM) di Rumah Sakit Bethesda Yogyakarta.

1.4.2 Sumber Data

Sumber data yang digunakan dalam penelitian ini diperoleh melalui observasi dan dokumentasi secara langsung terhadap proses pengelolaan file surat menyurat pasien pada bagian Surat Keterangan Medis (SKM) di Rumah Sakit Bethesda Yogyakarta.

1.4.3 Teknik Pengumpulan Data

Teknik pengumpulan data pada penelitian ini dilakukan menggunakan beberapa cara, diantaranya:

a. Observasi

Observasi dilakukan secara langsung pada bagian Surat Keterangan Medis (SKM) di Rumah Sakit Bethesda Yogyakarta untuk memperoleh informasi mengenai proses pengelolaan file surat menyurat pasien. Kegiatan observasi bertujuan untuk mengetahui alur pembuatan, penyimpanan, dan pengiriman dokumen secara elektronik serta kondisi keamanan dan kerahasiaan file yang dikelola oleh petugas.

b. Dokumentasi

Dokumentasi dalam penelitian ini dilakukan melalui pengambilan gambar atau *screenshot* pada proses pengelolaan file surat menyurat pasien di bagian SKM Rumah Sakit Bethesda Yogyakarta dengan izin dari pihak terkait. Dokumentasi yang dikumpulkan meliputi contoh formulir permohonan, kuitansi pembayaran, surat yang telah selesai dibuat, serta tampilan folder penyimpanan file surat menyurat pasien sebagai data pendukung untuk menggambarkan kondisi pengelolaan file surat menyurat pasien dan menjadi bahan pertimbangan dalam merancang prototipe sistem keamanan.