BAB 1

PENDAHULUAN

1.1 Latar Belakang

Rumah Sakit merupakan institusi pelayanan yang bergerak di bidang kesehatan yang bertujuan menyelenggarakan kegiatan kesehatan perorangan secara paripurna baik rawat jalan, rawat inap, dan gawat darurat (Ardianto et al., 2024). Rumah sakit merupakan organisasi yang bergerak di bidang kesehatan yang bertujuan untuk memenuhi kebutuhan pelayanan kesehatan di masyarakat (Prihadi & Meilani, 2020). Rumah Sakit merupakan institusi yang menyediakan pelayanan perawatan dengan menggunakan sarana dan prasarana, sumber daya manusia, dan teknologi (Algiffary et al., 2023).

RME merupakan rekam medis yang dibuat dan dirancang menggunakan sistem elektronik yang bertujuan untuk mengelola rekam medis dengan efektif dan efisien (Permenkes RI, 2022). Penggunaan RME memiliki peran yang penting guna meningkatkan kualitas sistem pelayanan kesehatan. Selain itu RME bertujuan untuk mengatasi tantangan seperti interoperabilitas. Beralihnya rekam medis manual ke rekam medis elektronik merupakan bagian dari berkembangnya teknologi khusunya di bidang kesehatan, dengan hadirnya RME dapat memudahkan dalam penggunaan serta memberikan manfaat yang banyak (Asih & Indrayadi, 2023).

Keamanan sistem informasi merupakan perlindungan terhadap akses, data, penggunaan, modifikasi, serta perlindungan terhadap ancaman yang datang dari internal maupun eksternal (Algiffary et al., 2023). Keamanan informasi adalah bagaimana menjaga aset informasi agar tetap rahasia, konsisten menjaga

penyimpanan, serta tepat dalam menjaganya (Marqonitatilla & Palupi, 2024). Tujuan dari keamanan informasi yaitu untuk menjaga keberlangsungan bisnis dan mengurangi ancaman dan bahaya yang akan berdampak dari insiden keamanan (Nurul et al., 2022).

Keamanan data pasien memiliki peran dan manfaat bagi sumber daya manusia dan rumah sakit tersebut. Data pasien akan terjaga dan terlindungi dari oknum yang tidak bertanggung jawab rumah sakit juga dapat meminimalisir kerugian finansial serta dapat meningkatkan kepercayaan masyarakat terkait keamanan informasi rumah sakit. Terlepas dari berbagai manfaat yang dapat dirasakan, tentunya terdapat ancaman yang harus diperhatikan. Pada Tahun 2020 di Indonesia terdapat kasus pencurian data kesehatan, sebanyak 230 ribu data pasien COVID-19 telah dicuri dan dijual. Selain itu pada Tahun 2022 sebesar 720 GB catatan pasien di beberapa rumah sakit dijual di forum *online* (Sofia et al., 2022). Sejalan dengan penelitian tersebut berdasarkan hasil wawancara di Rumah Sakit X diketahui bahwa petugas tidak mematikan komputer dan tidak *log out* akun petugas ketika selesai digunakan. Selain itu, beberapa petugas belum melakukan penggantian *username* dan *password* secara berkala, hal ini penting dilakukan untuk menjaga kerahasiaan data, apabila *username* dan *password* tersebut telah diketahui oleh pihak yang tidak berkepentingan (Ardianto et al., 2024).

Aman tidaknya data pasien dapat diukur dari beberapa aspek seperti kerahasiaan data pasien, integritas, ataupun ketersediaan data pasien. Dalam bidang kesehatan, keamanan dapat diukur menggunakan metode HIPAA (*Health Insurance Portability and Accountability Act*). Standar ini membahas sistem keamanan data

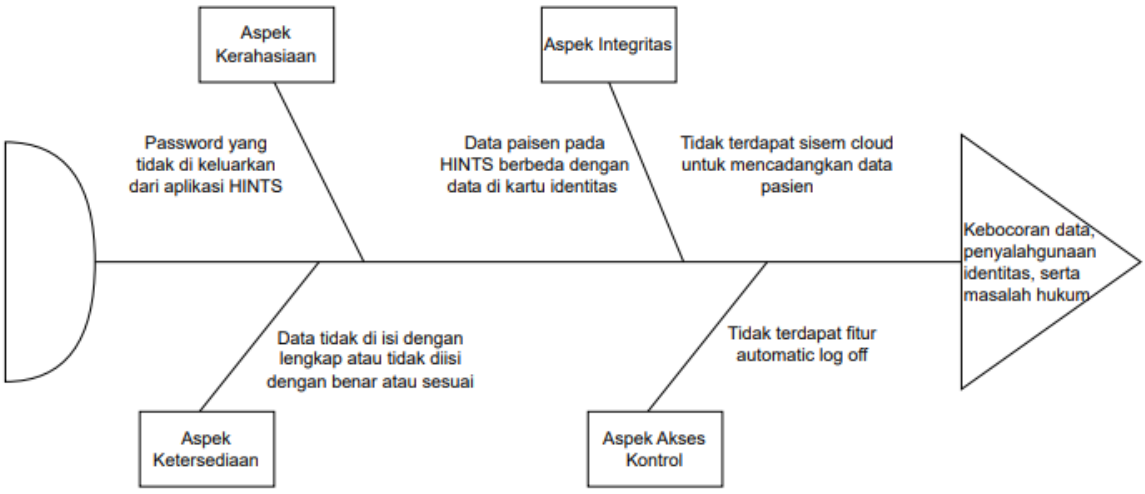
khususnya di bidang kesehatan, namun standar ini hanya berlaku untuk entitas yang dilindungi oleh departemen atau organisasi. Data perawatan kesehatan yang dihasilkan oleh entitas tidak dapat dilindungi oleh HIPAA (Moore & Frye, 2020). Selain itu, terdapat standar ISO/IEC 27001 yang memberikan penekanan terkait pemilihan kontrol harus didasarkan pada hasil serta kesimpulan yang diperoleh dari proses analisis dan penelitian risiko. Pada penelitian ini peneliti menggunakan standar ISO/IEC 27001 karena dapat meningkatkan keamanan informasi melalui penerapan *control* yang sistematis, serta dapat mengurangi risiko dengan mengidentifikasi dan mengelola risiko keamanan lebih efektif (Frangky & Sinaga, 2024).

Berdasarkan hasil *survey* awal yang dilaksanakan di Rumah Sakit Bhakti Dhrama Husada Surabaya pada tanggal 9 Januari 2025 terhadap salah satu petugas rekam medis rawat jalan terkait keamanan data pasien rekam medis elektronik di unit rawat jalan menyatakan bahwa terdapat beberapa masalah yang timbul dan dapat menyebabkan keamanan data pasien tergganggu seperti *password* telah tersimpan namun lupa dikeluarkan dari aplikasi RME rumah sakit yang bernama HINTS, tidak terdapat sistem *automatic log off*, data pasien yang tersimpan di HINTS tidak sesuai dengan kartu identitas pasien/kartu berobat pasien, tidak tersedianya sistem *back up* data atau *cloud* untuk menyimpan cadangan data pasien, serta data pasien tidak diisi dengan lengkap (nomor telefon diisi 000000000) atau diisi dengan lengkap namun tidak diisi dengan benar sehingga pada saat membutuhkan data pasien tidak tersedia.

Dari beberapa masalah tersebut, hal ini yang mendasari peneliti untuk memotret bagaimana keamanan data pasien rekam medis elektronik di Rumah Sakit Umum Daerah Bhakti Dharma Husada Surabaya, jika masalah tersebut terus dibiarkan terjadi rumah sakit akan memiliki tingkat risiko kebocoran data pasien yang tinggi, rumah sakit juga akan melanggar hukum mengenai pelanggaran privasi pasien, akan terjadi risiko kehilangan data secara permanen serta menurunnya kepercayaan masyarakat mengenai kualitas pelayanan rumah sakit.

Berdasarkan hal tersebut, peneliti melakukan penelitian yang berjudul "Gambaran Keamanan Data Pasien Rekam Medis Elektronik Pada Unit Rawat Jalan Berdasarkan Standar ISO/IEC 27001 Di Rumah Sakit Umum Bhakti Dharma Husada Surabaya" untuk meengidentifikasi potensi risiko kebocoran data serta upaya perlindungan guna menjaga keamanan data pasien RME unit rawat jalan.

1.2 Identifikasi Masalah



Gambar 1.1 Identifikasi Penyebab Masalah

Berdasarkan Gambar 1.1 menyatakan beberapa masalah terkait keamanan data pasien rekam medis elektronik di unit rawat jalan di Rumah Sakit Umum Daerah Bhakti Dharma Husada Surabaya adalah:

1. Aspek kerahasiaan

   Masalah yang ada pada aspek kerahasiaan yaitu password yang masih tersimpan di aplikasi "HINTS" sehingga terdapat *id user* dan *password* petugas yang masih terlihat. Tentu hal ini mengakibatkan oknum yang tidak bertanggung jawab dapat mengakses aplikasi tersebut.

2. Aspek integritas

   a. Masalah yang ada di aspek integritas yaitu data pada pasien pada aplikasi "HINTS" beberapa ada yang berbeda dengan kartu identitas atau kartu berobat pasien sehingga mengakibatkan perbedaan data antara kartu identitas dengan data yang ada di aplikasi.

   b. Tidak terdapat sistem *cloud* pada aplikasi "HINTS" sehingga menyebabkan data hilang dan bisa terhapus permanen.

3. Aspek ketersediaan

   Masalah yang ada di aspek ketersediaan yaitu data tidak diisi dengan benar atau lengkap sehingga menyebabkan kesulitan mencari data pasien serta menyebabkan duplikasi data.

4. Aspek akses kontrol

   Masalah yang ada di aspek akses kontrol yaitu tidak adanya fitur di aplikasi "HINTS" *automatic log off* sehingga ketika petugas meninggalkan computer yang belum ter *log off* orang lain bisa mengakses tanpa izin.

1.3 Batasan Masalah

Pada metode ISO/IEC 27001 terdapat 6 aspek indikator yang terdiri dari aspek kerahasiaan (*Confidentiality),* integritas (*Integrity*), autentifikasi (*Authentification*), akses kontrol *(access control)*, Non-Penyangkalan (*Non-Repudiation*), ketersediaan (*Availability*). Dalam penelitian ini difokuskan pada keamanan data pasien pada rekam medis elektronik berdasarkan metode ISO/IEC 27001 dari aspek kerahasiaan (*Confidentiality*) yang terdiri dari penerapan kata sandi, teknologi kriptografi, pemblokiran akses data. Aspek integritas (*Integrity*) yang berisi perubahan data dan pencadangan. Aspek autentifikasi (*Authentification*) tidak diteliti. Aspek tersedia (*Availability*) yang berisi efektivitas data dan efisiensi data. Aspek akses kontrol *(access control)* yang berisi penerapan *automatic log off*. Aspek Non-Penyangkalan (*Non-Repudiation*) tidak diteliti.

1.4 Rumusan Masalah

Berdasarkan uraian latar belakang, permasalahan yang akan ditinjau pada penelitian ini adalah bagaimana gambaran keamanan data pasien rekam medis elektronik pada unit rawat jalan berdasarkan Standart ISO/IEC 27001 di RSUD Bhakti Dharma Husada Surabaya?

1.5 Tujuan

1.5.1 Tujuan Umum

Tujuan penelitian ini untuk menggambarkan sistem keamanan data pasien rekam medis elektronik unit rawat jalan berdasarkan metode ISO/IEC 27001 di RSUD Bhakti Dharma Husada Surabaya.

1.5.2 Tujuan Khusus

1. Mengidentifikasi keamanan data pasien RME dari aspek kerahasiaan (*Confidentiality*)
2. Mengidentifikasi keamanan data pasien RME dari aspek integritas (*Integrity*)
3. Mengidentifikasi keamanan data pasien RME dari aspek ketersediaan (*Availability*)
4. Mengidentifikasi keamanan data pasien RME dari apek akses kontrol (*Acces control*)

1.6 Manfaat

1.6.1 Manfaat Bagi Peneliti

Penelitian ini bermanfaat untuk menambah pengetahuan dan pengalaman ilmu rekam medis di Rumah Sakit Bhakti Dharma Husada khususnya untuk mengetahui sistem keamanan data pasien.

1.6.2 Manfaat Bagi Rumah Sakit

Hasil penelitian yang dilakukan ini diharapkan dapat menjadi bahan masukan bagi rumah sakit dalam meningkatkan sistem keamanan data guna menciptakan kemanan yang baik dan terjaga khususnya di Rumah Sakit Bhakti Dharma Husada Surabaya.

1.6.3 Manfaat Bagi STIKES Yayasan Dr.Soetomo

Dapat digunakan sebagai bahan masukan dalam penerapan penelitian yang berkaitan dengan kemanan data serta sebagai bahan referensi perpustakaan guna kepentingan pengembangan ilmu pengetahuan tentang rekam medis rumah sakit.