RINGKASAN

Perkembangan teknologi informasi mendorong rumah sakit untuk beralih ke sistem digital dalam pengelolaan data medis. Namun, hal ini juga menghadirkan risiko terhadap keamanan data pasien yang bersifat sensitif. Berdasarkan hasil observasi dan wawancara, ditemukan beberapa permasalahan seperti penggunaan password sederhana, tidak adanya batasan percobaan login yang gagal, pengguna tidak mengganti password secara berkala, serta penempatan server utama dan cadangan dalam satu gedung.

Analisis menggunakan metode CIA (Confidentiality, Integrity, Availability) menunjukkan bahwa pada aspek *Confidentiality*, sistem belum optimal karena belum menerapkan kombinasi karakter password dan pembatasan percobaan login. Pada aspek *Integrity*, sistem telah mendukung keamanan melalui fitur log audit, verifikasi data, dan close billing otomatis untuk menjaga keakuratan dan keabsahan data pasien. Sedangkan pada aspek *Availability*, sistem hanya dapat diakses melalui jaringan internal dan telah memiliki server cadangan, namun diperlukan pembangunan Disaster Recovery Center (DRC) untuk memastikan ketersediaan data saat terjadi gangguan.

Sebagai bentuk solusi, dirancang fitur Notifikasi Pengingat Penggantian Password Otomatis untuk meningkatkan kedisiplinan pengguna dalam memperbarui kata sandi sesuai SPO SIMRS RSPAD. Rancangan ini diharapkan mampu memperkuat keamanan informasi sesuai dengan Permenkes No. 24 Tahun 2022 dan Peraturan BSSN No. 4 Tahun 2021, sehingga mendukung terwujudnya sistem informasi rumah sakit yang aman, andal, dan berkelanjutan.

Kata Kunci: Keamanan Informasi, SIMRS, Rekam Medis Elektronik, Confidentiality, Integrity, Availability, RSPAD Gatot Soebroto Puskesad, BSSN, Permenkes No. 24 Tahun 2022