BAB V

PENUTUP

A. Kesimpulan

1. Keamanan data RME berdasarkan aspek *confidentiality* belum sepenuhnya optimal. Sistem telah menerapkan login menggunakan *username* dan *password*, serta *automatic logout*. Namun, belum terdapat SPO kerahasiaan data, standar kompleksitas *password*, kewajiban penggantian *password* berkala, dan enkripsi data internal belum diterapkan secara menyeluruh, serta masih ditemukan penggunaan akun bersama.
2. Keamanan data RME berdasarkan aspek *integrity* telah berjalan namun masih memerlukan perbaikan. Sistem telah mengatur kewenangan dan batasan waktu pengeditan data, namun hanya menyimpan perubahan terakhir tanpa riwayat lengkap dan belum menerapkan validasi otomatis saat input data.
3. Keamanan data RME berdasarkan aspek *availability* secara umum sudah cukup baik. Sistem mudah diakses melalui jaringan khusus rumah sakit, didukung backup data terjadwal dan tiga lapisan server, serta akses dari luar rumah sakit dibatasi bagi pihak tertentu dengan VPN terdaftar. Namun, uji coba pemulihan data belum terjadwal dan SPO *recovery* belum tersedia.
4. Keamanan data RME berdasarkan aspek authentication telah menggunakan *username* dan *password* berbasis NIK Karyawan, namun masih bersifat *single factor*, belum menerapkan tanda tangan elektronik

karena keterbatasan sertifikasi dan biaya, serta masih ditemukan penggunaan akun bersama.

5. Keamanan data RME berdasarkan aspek *access control* telah mengatur hak akses sesuai peran, pencabutan akses otomatis bagi pegawai nonaktif, SPO pengajuan hak akses, serta notifikasi otomatis saat percobaan login gagal. Namun, evaluasi berkala hak akses belum konsisten dan masih ditemukan akun bersama serta *password* tersimpan di *browser*.
6. Keamanan data RME berdasarkan aspek *non-repudiation* telah memiliki fitur *audit trail* yang mencatat aktivitas pengguna dan tidak dapat diubah oleh pengguna biasa. Namun, riwayat perubahan data belum tercatat lengkap dan belum semua pengguna mengetahui fungsi fitur tersebut.

B. Saran

1. Bagi Rumah Sakit Nur Hidayah

   a. Aspek *Confidentiality*:

      Rumah sakit perlu menyusun dan menetapkan SPO kerahasiaan data pasien, menerapkan standar kompleksitas *password* (kombinasi huruf besar, huruf kecil, angka, dan simbol minimal 8 karakter), mengaktifkan sistem yang mewajibkan penggantian *password* secara berkala minimal setiap 6 bulan, mempercepat proses enkripsi data internal, serta memberikan edukasi rutin kepada seluruh petugas mengenai pentingnya menjaga keamanan akun masing-masing dan melarang penggunaan akun secara bersama.

b. Aspek *Integrity*:

Rumah sakit perlu mengembangkan sistem yang mampu merekam seluruh riwayat perubahan data secara lengkap, bukan hanya menyimpan perubahan terakhir. Selain itu, perlu diterapkan validasi otomatis saat *input* data untuk mencegah kesalahan, serta disusun SPO mengenai prosedur *editing* dan pencatatan histori perubahan data RME.

c. Aspek *Availability*:

Rumah sakit perlu menyusun SPO pemulihan data (*recovery*) dan menjadwalkan uji coba pemulihan data (*disaster recovery test*) secara rutin dan terstruktur, serta mendokumentasikan setiap insiden gangguan sistem agar dapat dijadikan bahan evaluasi berkelanjutan.

d. Aspek *Authentication*:

Rumah sakit perlu mengupayakan penerapan *multi-factor authentication* pada sistem RME, melakukan tanda tangan elektronik bagi tenaga kesehatan dan pasien sesuai regulasi yang berlaku, serta mempertegas kebijakan larangan penggunaan akun secara bersama disertai sanksi yang jelas.

e. Aspek *Access Control*:

Rumah sakit perlu melaksanakan evaluasi berkala terhadap kesesuaian hak akses pengguna secara konsisten dan terjadwal, menerapkan sistem notifikasi otomatis terhadap setiap upaya akses yang tidak sesuai kewenangan, serta memperketat mekanisme *role-based access control* untuk mencegah penyalahgunaan akses.

f. Aspek *Non-Repudiation*:

Rumah sakit perlu meningkatkan kapasitas fitur *audit trail* agar dapat mencatat seluruh riwayat aktivitas dan perubahan data secara rinci dan lengkap, memperluas akses *audit trail* kepada pihak-pihak yang berkepentingan secara terkontrol, serta mensosialisasikan fungsi dan manfaat *audit trail* kepada seluruh pengguna sistem RME.

g. Rumah sakit perlu meningkatkan kompetensi petugas melalui pelatihan berkala terkait keamanan data RME, serta meningkatkan keamanan sistem melalui pembaruan teknologi, perangkat, dan infrastruktur pendukung secara berkelanjutan.

2. Bagi Peneliti Selanjutnya

a. Meneliti mengenai tingkat pemahaman petugas terkait fitur keamanan pada sistem Rekam Medis Elektronik (RME) untuk mengetahui penerapan keamanan data di fasilitas pelayanan kesehatan.

b. Peneliti selanjutnya diharapkan dapat melibatkan informan dari berbagai unit pelayanan rumah sakit untuk memperoleh informasi yang lebih komprehensif mengenai penerapan keamanan data Rekam Medis Elektronik (RME).