BAB V

KESIMPULAN DAN SARAN

A. Kesimpulan

Kegiatan yang dilakukan oleh RS Bhayangkara Polda DIY dalam menjaga keamanan data pada Aplikasi SIMRS berdasarkan aspek yang diteliti adalah sebagai berikut:

1. Berdasarkan aspek *confidentiality* pada Aplikasi SIMRS di RS Bhayangkara Polda DIY telah diterapkan melalui *Role-Based Access Control* (RBAC), penggunaan akun sesuai jabatan, fitur *automatic logout*, serta SOP Keamanan dan Perlindungan Data SIMRS. Namun, masih ditemukan praktik *account sharing* antar petugas serta kepatuhan terhadap penggantian *password* secara berkala yang belum sepenuhnya terlaksana.
2. Berdasarkan aspek *integrity* pada Aplikasi SIMRS di RS Bhayangkara Polda DIY telah didukung melalui pembatasan hak akses perubahan data, *audit trail*, penerapan tanda tangan elektronik, pembatasan revisi data pasien selama tiga hari sebelum terkunci. Namun, akses terhadap *audit trail* masih terbatas pada petugas IT dan rumah sakit masih terus menggalakkan penggunaan tanda tangan elektronik untuk mengoptimalkan penggunaannya pada seluruh proses pelayanan.
3. Berdasarkan aspek *availability* pada Aplikasi SIMRS di RS Bhayangkara Polda DIY telah terintegrasi antar unit pelayanan secara *real-time*, *backup* data harian otomatis, server *backup* dan cadangan servernya, dan tersedianya SOP terkait *downtime* terencana dan tidak terencana. Namun,

masih ditemukan kendala berupa gangguan pada proses *bridging* data ke sistem eksternal (BPJS, IDRG, Satu Sehat), serta risiko kehilangan data saat terjadi pemadaman listrik mendadak akibat tidak tersedianya UPS di beberapa unit (Rekam Medis, Fisioterapi, Farmasi, Administrasi/Kasir).

B. Saran

1. Bagi Rumah Sakit Bhayangkara Polda DIY:
   a. Aspek *Confidentiality* (Kerahasiaan)

      Kepala unit perlu meningkatkan pengawasan kepatuhan pengguna SIMRS dalam menerapkan SOP Keamanan dan Perlindungan Data yang telah disosialisasikan, dan larangan *account sharing.* Menyusun dan menetapkan kebijakan penggantian *password* secara berkala sesuai kebijakan yang berlaku. Rumah sakit perlu melengkapi SOP yang sudah ada dengan prosedur penanganan insiden keamanan data dan tata cara penonaktifan akun pengguna yang berhenti bekerja.

   b. Aspek *Integrity* (Integritas)

      Kepala IT perlu mengoptimalkan fitur *audit trail* dan mempertimbangkan pemberian akses pemantauan kepada kepala unit sesuai kewenangan. Rumah sakit juga perlu terus menggalakkan penggunaan tanda tangan elektronik secara konsisten pada seluruh proses pelayanan yang memerlukan autentikasi digital dan evaluasi berkala terhadap integritas dan keamanan data SIMRS.

c. Aspek *Availability* (Ketersediaan)

Kepala IT perlu menyediakan *Uninterruptible Power Supply* (UPS) di setiap komputer yang digunakan untuk mengakses SIMRS. Meningkatkan stabilitas koneksi *bridging* data ke sistem eksternal (BPJS, IDRG, Satu Sehat) dan menyiapkan mekanisme alternatif apabila *bridging* mengalami gangguan. Melakukan monitoring dan evaluasi rutin terhadap sistem *backup* data.

2. Bagi Peneliti Selanjutnya:

Mengembangkan penelitian dengan mempelajari lebih dalam penerapan keamanan data RME berdasarkan konsep CIA Triad dan menambahkan Aspek *Authentication* (autentikasi) dan *Non-repudiation,* guna memperoleh gambaran keamanan data yang lebih komprehensif. Melakukan penelitian di Rumah Sakit lain dengan jenis dan tingkat yang berbeda untuk membandingkan implementasi keamanan data RME lintas institusi serta mengidentifikasi praktik terbaik yang dapat diadaptasi.