BAB V

PEMBAHASAN

A. Faktor-Faktor yang Mempengaruhi Keamanan Data Pasien pada Rekam Medis Elektronik

Keamanan dari Rekam Medis Elektronik harus terjaga dengan baik sehingga informasi data pasien tidak terjadi kebocoran dan disalah gunakan bagi pihak yang kurang bertanggung jawab. Setelah mereview 5 jurnal, pada jurnal 3 dijelaskan untuk RME wajib memliki fitur-fitur yang lengkap misalnya seperti *User ID* serta *password* untuk keamanan dan akses ke data rekam medis elektronik agar tidak sembarang orang yang dapat mengakses informasi pasien. Keamanan suatu sistem informasi juga dapat dipengaruhi oleh pihak luar yang tidak bertanggung jawab seperti yang disinggung pada jurnal 2, alasan bahwa keamanan informasi pada sektor kesehatan harus menjadi prioritas diantaranya karena teknik pencurian data oleh hacker semakin bervariasi, teknik perlindungan data pasien semakin kompleks, meningkatnya kasus penyanderaan data melalui *ransomware*, risiko dari pihak ketiga, kerawanan e-mail serta aplikasi bergerak (mobile application) maka dari itu perlunya keamanan sistem yang lebih baik untuk mencegah kejadian tersebut.

Perubahan data pada Rekam Medis Elektronik pasien tidak dapat diubah tanpa izin dokter. Jurnal 1 menjelaskan perubahan data, tetapi tidak ada tanda tangan elektronik dari dokter gigi pada rekam medis elektronik. Akses pada sistem informasi kesehatan juga harus diperjelas batasannya agar hanya petugas yang berwenang yang dapat menghapus atau mengedit data seperti yang sudah dijelaskan pada jurnal 4 sedangkan pada jurnal 5 dibahas mengenai SDM yang menggunakan RME menunjang keberhasilan penggunaan Rekam Medis Elektronik maka petugas yang menggunakan RME berpengarung juga dalam menjaga keamanan data pasien pada RME

UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA PERPUSTAKAAN

B. Mengantisipasi Kebocoran Data Rekam Medis Elektronik Melalui Aspek Keamanan

1. Aspek *Privacy or Confidentiality*

   Dalam Rekam Medis Elektronik cara mengantisipasi kebocoran data pasien melalui aspek *Privacy* menurut (Vinta et al., 2022) Kepemilikan informasi pribadi pasien serta sistem keamanan ini menggunakan hak akses terbatas seperti mempunyai *User ID* serta kata sandi agar menjamin *privacy*. Kemudian penggunaan teknologi kriptografi untuk mengakses informasi pada rekam medis elektronik serta setiap rumah sakit mempunyai firewall hingga arsip dokumen untuk melindungi dari kebocoran data.

2. Aspek *Integrity*

   Penggunaan antivirus juga berfungsi untuk mencegah kebocoran data, menurut (Wahyuningsih Nugraheni, 2017) Sistem pada RSUD Dr. Soediran Mangun Sumarso mempunyai 2 program antivirus yang diperbarui secara rutin, SMADAV serta AVAST. Antivirus tersebut dipakain untuk mengantisipasi virus yang datang dari Internet atau USB. Update antivirus yang normal ini sesuai dengan manfaat antivirus yaitu fungsi proteksi atau perlidungan data dari virus, dikarenakan virus selalu muncul yang baru atau *update*, oleh karena itu software antivirus juga perlu diupdate secara berkala.

3. Aspek *Authentication*

   Pada aspek *Authentication* disarankan dalam *password* dari *user id* petugas menggunakan kombinasi pada alfanumerik. Menurut (Wahyuningsih Nugraheni, 2017) Disarankan agar kata sandi tidak lebih dari 8 karakter ataupun kurang dari 6 karakter dan dikombinasikan dengan karakter alfanumerik. Juga, kata sandi minimal harus disediakan, karena akan sulit bagi peretas untuk menemukan kata sandi yang dipakai. Kata sandi administrator

UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA PERPUSTAKAAN

sistem informasi tidak ditentukan oleh tanggal kedaluwarsa, maka dari itu *user* selalu menggunakan kata sandi asli yang dibuat oleh administrator.

4. Aspek *Availability*

Ketersediaan informasi serta fasilitas dalam pelayanan juga mendukung keamanan data. Menurut (Tiorentap & Hosizah, 2020) kemudahan akses oleh *user* dimanapun, kapanpun, serta oleh siapapun yang mempunyai *user id & password*, serta dapat terhubung dengan koneksi internet. Dengan begitu dalam memastikan ketersediaan semua informasi kesehatan yang dilindungi yang dilindungi dalam membuat, menerima, mempertahankan, atau mentransmisikan informasi kesehatan sudah terpenuhi.

5. Aspek *Access Control*

Pembatasan akses dalam RME diperlukan karena hanya petugas yang bertanggung jawab yang bisa mengakses data pasien. Menurut (Vinta et al., 2022) bahwa mengizinkan pihak berwenang untuk menggunakan kombinasi yang berbeda dari kata sandi identifikasi pengguna untuk setiap orang ataupun untuk memblokir akses ke pengguna melalui mekanisme lain jika terjadi masalah otentikasi dan informasi abnormal tentang koneksi serta login menggunakan *ID* dan kata sandi.

6. Aspek *Non-Repudiation*

Pada aspek ini untuk mengatasi ketidakjujuran petugas yang salah dalam mengisi atau menghapus data pasien dilihat melalui riwayat perubahan data. Menuut (Pahlevi et al., 2021) Aspek non-rapadiatum, jadi tidak ada yang bisa menyangkal dalam memasukkan data. Kesalahan dalam penulisan rekam medis elektronik dapat ditemukan dengan melalui riwayat data yang dimasukkan. Jika terjadi perubahan data, maka dari itu riwayat data

UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA PERPUSTAKAAN

akan disimpan dan tidak dapat dihapus pada yang ditulis ke rekam medis elektronik RSIGM Sultan Agung Semarang.

PERPUSTAKAAN
UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA