BAB IV
PEMBAHASAN

1. Deskripsi Keamanan Informasi Elektronik dari berbagai Jurnal

Keamanan menurut Hatta (2013) merupakan suatu proteksi informasi pelayanan kesehatan serta kerusakan, kehilangan atau juga pengubahan data yang diakibatkan karena ulah pihak yang tidak bertangggung jawab. Sedangkan Mufadhol (2009) Keamanan diartikan sebagai salah satu aspek penting yang harus diperhatikan. Informasi baik berupa teks, gambar, audio,maupun video yang menyimpan asset penting, wajib dilindungi dengan sistem manajemen keamanan informasi. Kebocoran, kerusakan atau hilangnya suatu informasi dapat menimbulkan kerugian baik secara finansial maupun produktivitas. Penyimpanan yang aman bisa disebut sebagai penyimpanan yang meliputi keamanan terhadap pencurian, kebakaran, bencana alam juga kerusakan lain.

Menurut Badan Siber dan Sandi Negara (2019) menyebutkan bahwa Privasi dan Keamanan terhadap Pelindungan suatu data rekam medis pasien merupakan bagian dari kualitas pelayanan kesehatan. Data rekam medis yang disimpan dan didistribusikan secara elektronik akan renta disalah gunakan sehingga dapat merugikan pasien. Data rekam medis pasien harus terjaminaman, baik dari aspek privasi maupun keamanannya. Aspek privasi melindungi data rekam medis melalui mekanisme pengelolaan data pasien mulai dari proses pengumpulan data, kualitas data, dan kendali akses terhadap data tersebut. Aspek keamanan melindungi data rekam medis melalui jaminan kerahasiaan, integritas, dan ketersediaan datanya.

Berdasarkan Kementerian Kesehatan (2013) tentang SIMRS, keamanan SIMRS harus meliputi:

1. Keamanan fisik mencakup kebijakan hak akses pada ruang data *center*/server dan penggunaan hak akses komputer untuk user pengguna.

UNIVERSITAS JENDERAL ACHMAD YANI
PERPUSTAKAAN
YOGYAKARTA

2. Keamanan jaringan dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Tugas keamanan jaringan dikontrol oleh administrator jaringan. Segi-segi keamanan didefinisikan sebagai berikut:

   a) Informasi (data) hanya bisa diakses oleh pihak yang memiliki wewenang.

   b) Informasi hanya dapat diubah oleh pihak yang memiliki wewenang.

   c) Informasi tersedia untuk pihak yang memiliki wewenang ketika dibutuhkan. Pengirim suatu informasi dapat diidentifikasi dengan benar dan ada jaminan bahwa identitias yang didapat tidak palsu.

Berdasarkan *review* dari berbagai jurnal yang telah didapat adalah menurut Lerisa Desti Irlaili, Rohmadi (2018) menjelaskan bahwa keamanan data yang berhubungan dengan *Privacy* sistem yang ada sudah terintegrasi dimana hak akses antar sistem hanya sebatas data yang diperlukan oleh sistem yang ada dibagaian tersebut saja yang akan ditampilkan, Sedangkan unuk *fiture* keamanan data *Integrity* berkaitan dengan informasi yang tersedia hanya diubah dan diolah unk kebutuhan tertentu dan oleh pengguna tertentu yang berhak. Fitur Keamanan Data *authentication* berkaitan dengan cara untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud setiap pengguna sistem informasi sudah memiliki *username* dan *password* sendiri-sendiri.

Menurut Badan Siber dan Sandi Negara (2019) Keamanan informasi bukan hanya masalah dari sisi teknologi saja melainkan masalah sumber daya manusia juga. Manusia sebagai aktor yang menjalankan teknologi, merupakan salah satu ancaman keamanan terbesar untuk berbagai sektor, termasuk kesehatan. Sebagian besar pelanggaran keamanan diakibatkan oleh faktor manusia. Kelalaian atau kesalahan manusia yang sederhana dapat berdampak fatal bagi penyedia layanan kesehatan. *Phishing* merupakan salah satu teknik yang sering digunakan dan cukup efektif, dilakukan dengan memanfaatkan “ketidak pahaman” personil untuk mengklik tautan berbahaya.

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

Dalam suatu Organisasi kesehatan wajib melaksanakan program kesadaran keamanan informasi dan pelatihan wajib berkala bagi seluruh personil untuk menyadari pentingnya pelindungan data pribadi yang dikelola oleh organisasi

Hendri Nurvianto Saputra, Jamroni (2017) menjelaskan bahwa Pengetahuan petugas mengenai sistem keamanan ini didapatkan dari pengalaman mereka bekerja dan apa yang mereka lihat selama pemakaian SIMPUS di puskesmas. Petugas tidak mempelajari sistem keamanan lebih mendalam lagi, sehingga pada tahap aplikasi *(Aplication)* pelaksanaannya masih saja ada petugas puskesmas yang bebas memberikan *password* kepada orang lain. . Dengan tidak adanya batasan akses di puskesmas Pleret maka koordinator sistem informasi harus bertanggung jawab atas segala sesuatu yang telah dipilihnya dengan segala risiko, karena koordinator sistem informasi yang bertanggung jawab terhadap *password* data *server*.

Menurut Badan Siber dan Sandi Negara (2019) menjelaskan bahwa Organisasi kesehatan perlu mendefinisikan jenis data pribadi apa saja yang dikumpulkan dan disimpan dalam sistem, untuk tujuan penggunaan apa, bagaimana cara pengumpulannya, disimpan dimana, siapa saja yang bisa mengaksesnya, serta untuk berapa lama data tersebut disimpan. Sebaiknya dibentuk satu unit khusus yang bertanggung jawab penuh soal pelindungan data pribadi termasuk melakukan proses audit ini. Perlu juga memiliki data *inventory* yang mencatat arus keluar masuk data dalam sistem. Dapat juga menggunakan fitur "jejak audit", yang mencatat siapa yang mengakses informasi Anda, perubahan apa yang dilakukan dan kapan..

Cara Menjaga Informasi Agar Tidak Dirubah Puskesmas Pleret menggunakan *password* untuk menjaga informasi data server dari perubahan tanpa ada seizin pemilik informasi. Dalam pengendalian teknis di Puskesmas Pleret telah menggunakan cara yaitu dengan menggunakan sistem *back-up* data yang dilakukan rutin setiap bulan oleh koordinator sistem informasi supaya data yang ada ter *copy*. Namun cara ini dirasa kurang efektif mengingat kebocoran atau kerusakan terhadap data dapat terjadi sewaktu

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

waktu maka back up data dapat dilakukan secara periodic pada malam hari atau ketika selesai pelayanan mengendalikan, mengawasi dan menyelesaikan permasalahan yang berkaitan dengan *server* SIMPUS. Karena puskesmas Pleret tidak mempunyai prosedur sistem keamanan, maka dalam pengendalian, formal ini dilakukan dengan adanya koordinator sistem informasi manajemen puskesmas, dimana koordinator ini mempunyai tugas.

Menurut Badan Siber dan Sandi Negara (2019) Penyedia layanan kesehatan perlu melakukan sesi penilaian risiko secara teratur untuk menentukan kerentanan sistem miliknya. Identifikasi celah keamanan dapat mencegah insiden yang mungkin timbul. Penilaian risiko keamanan dilakukan per tahun atau ketika terjadi perubahan pada sistem elektronik.

Dea Anjani, Dr. Apol Pribadi Subriadi, S.T, M.T, Anisah Hediyanti, S.Kom, M.Sc (2015) menjelaskan Untuk risiko yang paling banyak terjadi terdapat pada *aset people* dengan risiko penyalah gunaan hak akses. Dari proses penilaian risiko menggunakan metode FMEA(*Failure Mode & Effect Analysis*) didapatkan risiko yang mempunyai skor assessment tertinggi hingga terendah. Untuk risiko very high dengan nilai RPN (*Risk Priority Number*) sebesar 392, yaitu pada kategori risiko people dengan identifikasi risiko Penyalahgunaan hak akses dan untuk risiko paling rendah dengan nilai RPN 18 terdapat pada risiko *Backup data failure.* Dari hasil penilaian risiko menggunakan metode FMEA(Failure Mode & Effect Analysis, maka diberikan penanganan atau tindakan pengendalian risiko untuk mengontrol risiko-risiko tersebut. Tindakan pengendalian untuk semua risiko-risiko tersebut mengacu pada ISO 27002 yang berfokus pada standarisasi Sistem Manajemen Keamanan Informasi (SMKI).

2. Presentase Keamanan Informasi Elektronik dari berbagai Jurnal

Berdasarkan hasil analisis jurnal Rasim, Mayadi (2016) Sebanyak 35 responden atau 72.92% menyatakan bahwa dalam memperbaiki kesalahan pada sistem informasi rekam medis saat ini sangat mudah dan mudah, sedangkan yang menyatakan kurang mudah (agak sulit) sebesar 12 responden

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

atau 25% dan yang menyatakan sulit dan sangat sulit sebanyak 2.08% Dari aspek Efisiensi sebagian besar responden yaitu 89.58% menyatakan sangat baik dan baik dan hanya 10.42% responden menyatakan kurang baik dan tidak baik Indikator lain yang digunakan untuk mengukur aspek ini adalah Reliabilitas yaitu Apakah sistem yang ada dapat dipercaya oleh pengguna untuk melakukan pekerjaan yang diminta. Sebanyak 43 responden atau 89.58%menyatakan bahwa sistem yang sangat dipercaya oleh pengguna untuk melakukan pekerjaan yang diminta, dan hanya 3 responden atau 6.25% menyatakan bahwa sistem informasi rekam medis ini kurang dapat dipercaya untuk melakukan pekerjaan yang diminta, dan 4.16% responden menyatakan bahwa sistem ini tidak dapat dan sangat tidak dapat dipercaya Aspek lain yang diukur adalah Kesederhanaan yaitu Seberapa sulitkah sistem ini dipahami oleh pengguna. Sebanyak 43 responden atau 89.58% menyatakan bahwa sistem informasi ini sangat mudah untuk dipahami oleh pengguna, dan hanya 10.42% pengguna menyatakan kurang mudah dan sulit untuk memahami sistem informasi ini Aspek berikutnya yang diukur adalah Kemudahan yaitu Apakah sistem informasi rekam medis ini dapat membantu mempermudah dalam memberikan penjelasan kepada pengguna. Sebanyak 43 respoden atau 89.58% responden menyatakan bahwa sistem informasi ini sangat mempermudah dalam membantu memberikan penjelasan kepada pengguna (pasien), dan sebanyak 3 responden atau 6.25% responden menyatakan bahwa sistem informasi ini kurang dapat membantu dalam memberikan penjelasan kepada pengguna (pasien), serta 4.16% responden menyatakan bahwa sistem informasi ini sulit dan sangat sulit dalam membantu dalam memberikan penjelasan kepada pengguna (pasien).

PERPUSTAKAAN UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA

PERPUSTAKAAN
UNIVERSITAS JENDERAL ACHMAD YANI
YOGYAKARTA