RAMMIK : Jurnal Rekam Medik dan Manajemen Informasi Kesehatan
Vol. 1, No. 2, Oktober 2022, hlm. 94 - 103
EISSN: 2829-4777
URL : https://rammik.pubmedia.id/index.php/rmik

Analisis Aspek Keamanan Informasi Pasien Pada Penerapan RME di Fasilitas Kesehatan

Siti Sofia[1], Efri Tri Ardianto[2], Niyalatul Muna[3], Sabran[4]
[1,2]Manajemen Informasi Kesehatan, Kesehatan, Politeknik Negeri Jember
Sitisofia2108@gmail.com, Efritriardianto@polije.ac.id, Niyalatul@polije.ac.id, Sabran@polije.ac.id

Keywords:
EMR,
Health facilities,
Literature review,
Security aspect

ABSTRACT
Data security issues are becoming increasingly serious as the trend of data theft is increasing. This causes not only material losses but also psychological victims. The purpose of this study was to determine how the information security of patient data in the application of RME in terms of information security aspects. The method used is a literature review by analyzing 20 articles from various sources. The results of the study show that from the articles reviewed in terms of 6 security aspects, namely username and password, changes or deletions of data by administrators, electronic signatures and the use of PINs, aspects of using data backup processes to anticipate patient data hacking, restrictions on access rights by using user id & password for each user, as well as log file usage. Overall, health facilities basically have carried out data security on the information systems they use, but in practice there are still health facilities that do not fully meet the data security aspect or are not optimal in using the techniques used. System managers need to develop techniques or ways to secure data more optimally that can fulfill 6 aspects of information security in electronic medical records.

Kata Kunci
Aspek keamanan,
Fasilitas kesehatan,
Literature review,
RME

ABSTRAK
Masalah keamanan data menjadi semakin serius karena tren pencurian data semakin meningkat. Hal ini menyebabkan kerugian bukan hanya materil tetapi juga psikis korban. Tujuan dari penelitian ini adalah mengetahui bagaimana keamanan informasi data pasien pada penerapan RME ditinjau dari aspek keamanan informasi. Metode yang digunakan adalah *literature review* dengan menganalisis 20 artikel dari berbagai sumber. Hasil penelitian menunjukkan dari artikel yang dilakukan review yang ditinjau dari 6 aspek keamanan yaitu *username* dan *password*, perubahan atau penghapusan data oleh administrator, adanya tanda tangan elektronik dan penggunaan PIN, Aspek menggunakan proses *backup* data guna mengantisipasi peretasan data pasien, pembatasan hak akses dengan penggunaan *user id & password* bagi masing-masing pengguna, serta penggunaan *log file*. Secara keseluruhan, fasilitas kesehatan pada dasarnya telah melakukan pengamanan data pada sistem informasi yang digunakannya, namun dalam penerapanya masih terdapat fasilitas kesehatan yang tidak sepenuhnya memenuhi aspek keamanan data atau belum maksimal dalam menggunakan teknik yang digunakan. Pengelola sistem perlu melakukan pengembangan teknik atau cara mengamankan data dengan lebih maksimal yang dapat memenuhi 6 aspek keamanan informasi pada rekam medik elektronik.

Korespondensi Penulis:

Siti Sofia,
Politeknik Negeri Jember,
Jl. Mastrip 164 Jember
Telepon : +6282257140231
Email: alifa.luvian@gmail.com

1. PENDAHULUAN

Fasilitas Kesehatan adalah suatu alat dan/atau tempat yang digunkan untuk menyelenggarakan upaya pelayanan kesehatan, baik promotif, preventif, kuratif maupun rehabilitatif yang dilakukan oleh pemerintah pusat, pemerintah daerah, dan/atau masyarakat [1] . Salah satu dokumen yang penting dalam fasilitas kesehatan disebut dengan dokumen rekam medis. Suatu berkas yang berisikan catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan, dan pelayanan lain yang diberikan kepada pasien pada suatu fasilitas kesehatan merupakan suatu dokumen yang disebut dengan rekam medis [1]. Rekam medis wajib disimpan dan dijaga kerahasiaannya oleh dokter atau dokter gigi dan pimpinan sarana layanan kesehatan. Pencatatan rekam medis wajib bagi dokter dan dokter gigi yang melakukan tindakan medis kepada pasien [3]. Berdasarkan pada peraturan tersebut sehingga tidak ada alasan bagi dokter atau dokter gigi untuk tidak membuat rekam medik pasien.

Salah satu penerapan Teknologi Informasi (TI) di Indonesia pada bidang kesehatan disebut dengan Rekam Medik Elektronik (RME). Sarana pelayanan kesehatan dapat menyelenggarakan rekam medik elektronik [5].Penyelenggaraan rekam medik dengan menggunakan teknologi informasi elektronik diatur lebih lanjut dengan peraturan tersendiri. Suatu informasi harus berbentuk tertulis atau asli, informasi elektronik dan atau dokumen elektronik dikatakan sah jika informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan [6].

Masalah keamanan data menjadi semakin serius karena tren pencurian data menjadi meningkat. Di Indonesia, kasus pencurian data kesehatan bukan hal yang baru. Pada tahun 2020, data 230 ribu pasien COVID-19 di Indonesia diduga telah dicuri dan dijual. Hal ini menyebabkan kerugian tidak hanya materil tetapi juga psikis korban, dimana mereka bisa saja mendapatkan perlakuan diskriminasi di lungkungan masyarakat [8]. Pada bulan januari tahun 2022, terdapat juga dugaan kebocoran data catatan medis pasien di sejumlah rumah sakit di Indonesia. data berukuran 720 GB itu dijual di forum online Raidforums [9].

Prinsip Keamanan informasi khususnya dalam bidang kesehatan mencakup enam aspek yaitu *privacy*, *integrity*, *authentication*, *availability*, *access control* dan *non repudiation* [10]. Berdasarkan penelitiaan yang dilakukan di RSUD dr. Moewardi diperoleh hasil bahwa di rumah sakit tersebut belum terdapat fasilitas tanda tangan elektronik, hal itu tidak sesuai dengan aspek *authentication* [11]. Berdasarkan aspek *integrity*, rekam medik elektronik pada Rumah Sakit dr. Moewardi juga belum memfasilitasi perubahan informasi dimana pencoretan/penghapusan tidak dapat dilakukan. Hal tersebut dapat meingkatkan resiko ketidakamanan rekam medis dari pihak yang tidak bertanggung jawab.

Berdasarkan penelitian pada klinik Medical *Check-Up* ditemukan bahwa terdapat ketidaksesuaian prinsip keamanan sistem informasi yakni antar *user* masih saling bertukar informasi terkait *user-id* dan *password-nya.* Selain itu, satu user-id digunakan oleh beberapa orang juga sangat biasa dilakukan [10]. Hal tersebut tidak sesuai dengan aspek *Access control* dimana aspek tersebut menekankan pada cara pengaturan pembatasan hak akses terhadap informasi. Hal ini tentu saja akan berakibat fatal jika terjadi kesalahan penginputan, dimana menyulitkan untuk proses identifikasi pelaku. Jika hal tersebut terus berlanjut, dikhawatirkan akan mengakibatkan pada penggunaan informasi oleh pihak-pihak yang tidak bertanggung jawab.

Berdasarkan latar belakang yang telah dipaparkan, mengingat pentingnya fasilitas kesehatan dalam menjaga keamanan data pribadi pasien dalam pelaksanaan rekam medis elektronik, serta dampak yang ditimbulkan apabila informasi dalam rekam medis pasien bocor dan berisiko akan digunakan oleh pihak yang tidak bertanggungjawab, peneliti tertarik melakukan penelitian dengan judul "Analisis Aspek Keamanan Informasi Data Pasien Pada Penerapan Rekam Medik Elektronik Di Fasilitas Kesehatan (*Literature Review*)" untuk mengetahui lebih lanjut bagaimana implementasi rekam medik elektronik di fasilitas kesehatan

2. METODE PENELITIAN

Metode penelitian yang digunakan adalah *literature review*. *Literature review* merupakan metodologi penelitian yang bertujuan mengumpulkan dan mengambil inti dari penelitian sebelumnya serta menganalisis beberapa *overview* para ahli yang tertulis dalam teks. *Literature-review* memiliki peran sebagai landasan untuk berbagai jenis penelitian karena hasil *literature review* memberikan pemahaman tentang perkembangan pengetahuan, sumber stimulus pembuatan kebijakan, memantik penciptaan ide baru dan berguna sebagai panduan untuk penelitian bidang tertentu. *Literature review* dilakukan dengan cara menganalisis, menyintesis, meringkas, dan membandingkan hasil-hasil penelitian yang satu dengan lainnya.

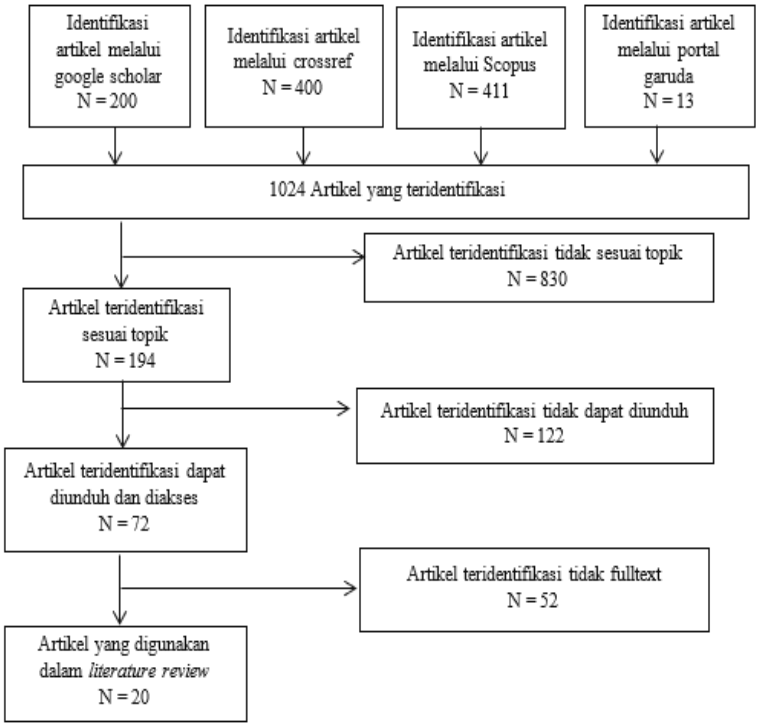
2.1 Metode Pengumpulan Data

Data yang digunakan dalam penelitian ini adalah hasil penelitian yang telah dilakukan oleh peneliti-peneliti terdahulu. Sumber data dapat berupa buku, artikel penelitian, maupun laporan ilmiah. Pencarian *literature* dilakukan pada database online yang memiliki *repository* besar dan *free data source* seperti *Google Scholar, Crossref, Scopus,* dan Portal Garuda.

2.2 Pencarian Literature dan Temuan Artikel

Pencarian artikel pada database online *Google Scholar, Crossref,* Portal Garuda dan *Scopus* dilakukan menggunakan aplikasi *Publish or Perish.*artikel yang digunakan adalah artikel yang telah memenuhi kriteria inklusi dan eksklusi meliputi Artikel membahas mengenai masalah keamanan data pasien pada rekam medik elektronik, Artikel dapat diakses dan diunduh, Artikel tidak terbatas penelitian (kualitatif, kuantitatif, dan *mix method),* Artikel dengan terbitan tahun 2012 – 2022.

Berikut merupakan proses pencarian dan seleksi artikel:



Gambar 1. Alur Penemuan Artikel

3. HASIL DAN ANALISIS

3.1 Hasil Identitifkasi Artikel

Hasil identifikasi data literatur melalui *Crossref* sebanyak 1024 data artikel melalui database *Crossref* ditemukan 400 artikel, *Google Scholar* sebanyak 200 artikel, Portal Garuda sebanyak 13 artikel, dan Scopus sebanyak 411 artikel. Selanjutnya diseleksi berdasarkan kriteria inklusi dan esklusi yang telah ditentukan dan diperoleh sebanyak 20 (dua puluh) artikel untuk digunakan. Berikut merupakan hasil *temuan* artikel ditinjau dari 6 aspek keamanan informasi.

Tabel 1. Ekstraksi Data

No.	Aspek Keamanan	*Author*
1.	*Privacy*	[12], [2], [5], [15], [16], [17], [18], [19], [20], [21], [22]
2.	*Integrity*	[12], [13], [14], [18], [21], [23], [24], [22], [25]

3.	*Authentication*	[2], [4], [5], [9], [12], [13], [14], [15], [17], [18]
4.	*Availability*	[12], [13], [17], [21], [23], [28]
5.	*Acces control*	[2], [4], [5], [6], [7], [8], [9], [10], [12], [14], [19]
6.	*Non-repudiation*	[12]–[14], [16], [21], [22]

3.2 Penerapan Aspek *Privacy* Pada Rekam Medik Elektronik Di Fasilitas Kesehatan

Privacy atau *confidentiality* adalah penjagaan informasi dari pihak-pihak yang tidak memiliki hak untuk mengakses informasi. Data rekam medis yang disimpan dan didistribusikan secara elektronik akan rentan disalah gunakan sehingga dapat merugikan pasien. Data rekam medis pasien harus terjamin aman, 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.

Berdasarkan artikel yang telah di review ditemukan beberapa teknik yang digunakan fasilitas kesehatan untuk menjaga keamanan rekam medik elektronik dalam menjamin aspek *privacy* yaitu penerapan login dengan *username* dan *password*, penerapan *automatic log off*, teknologi kriptografi, serta pemblokiran akses ke data menggunakan teknologi jaringan. Hasil review artikel yang telah ditemukan, sebagian besar artikel membahas mengenai penerapan keamanan rekam medik elektronik dengan menerapkan login *username* dan *password*. *Username* dan *password* digunakan untuk membuktikan bahwa pengguna memiliki wewenang untuk memakai dan masuk ke dalam sistem. Oleh karena itu setiap pengguna sebelum masuk ke dalam sistem informasi harus mengetik/memasukkan *username* beserta *password*. Untuk menghindari percobaan pengaksesan oleh pengguna yang tidak memiliki wewenang, harus dikontrol dengan mengkombinasikan kontrol preventif dan pendeteksian.

Sistem informasi yang digunakan telah menjamin aspek *privacy* yang dibuktikan dengan adanya penerapan login dengan *username* dan *password*. Keamanan informasi bukan hanya masalah dari sisi teknologi saja, melainkan juga masalah sumber daya manusia itu sendiri. 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 timbul kelalaian atau kesalahan manusia yang sederhana dan berdampak fatal bagi penyedia layanan kesehatan. Penerapan *username* dan *password* saja tidak cukup untuk menjaga keamanan data pasien tanpa adanya kesadaran oleh pengguna terkait keamanan data, karenanya perlu adanya pemahaman tentang kesadaran keamanan oleh pengguna sistem informasi supaya informasi tersebut dapat terjaga. Pentingnya pemahaman tentang keamanan informasi demi menjaga data privasi dan meminimalisasi tindak kejahatan siber atau kejahatan dunia maya dan masalah keamanan informasi lainnya. Hal itu dapat menyebabkan banyak sekali kasus rekam medis yang digunakan untuk tujuan selain kepentingan pelayananan kesehatan. Rekam medik elektronik juga berisiko tinggi mengalami kebocoran karena dapat diakses secara luas oleh banyaknya petugas yang harus merawat pasien yang sama.

Selain mendorong pengguna untuk menjaga keamanan, sistem informasi sebaiknya disediakan juga fitur yang memungkinkan pengguna keluar atau logout otomatis jika mereka tidak melakukan aktivitas apapun selama durasi waktu tertentu. Hal ini sangat penting untuk mencegah orang yang tidak berhak menggunakan sistem informasi tersebut, jika pengguna meninggalkan komputer dalam waktu relatif lama. Aspek *privacy* dibuktikan dengan bentuk tidak aktifnya (melakukan *log-out* secara otomatis) sistem informasi klinik jika dalam kurun waktu 5 (lima) menit tidak terjadi aktivitas yang dilakukan oleh *user*.[10]. Hal ini berfungsi sebagai bentuk pertahanan ataupun pencegahan dari bentuk penyalahgunaan *user id*.

Aspek *privacy* sudah banyak diterapkan dalam menjamin keamanan data pasien pada rekam medik elektronik di fasilitas pelayanan kesehatan. Dengan banyaknya fasilitas kesehatan yang telah menerapkan aspek *privacy* maka tingkat keamanan data akan semakin tinggi karena telah dilakukan pencegahan bagi pihak yang tidak berhak untuk mengakses informasi yang tersimpan dalam rekam medik elektronik. Sehingga pasien sebagai pemilik data tidak perlu khawatir bahwa datanya akan diakses oleh pihak yang tidak berhak atau tidak diberi ijin untuk mengakses.

3.3 Analisis Aspek Integrity Pada Penerapan Rekam Medik Elektronik di Fasilitas Kesehatan

Integrity merupakan aspek yang berkaitan dengan perubahan informasi, segala bentuk perubahan yang dilakukan pada sistem atau rekam medik elektronik, dapat diketahui oleh sistem yang ada. Pembetulan hanya dapat dilakukan dengan cara pencoretan tanpa menghilangkan catatan yang

dibetulkan dan dibubuhi paraf dokter, dokter gigi atau tenaga kesehatan tertentu yang bersangkutan [5]. Pencoretan tentu saja tidak bisa dilakukan dalam rekam kesehatan elektronik. Oleh karena itu diperlukan pengamanan atau proteksi yang lebih yaitu tidak begitu saja menghapus data yang tersimpan dalam rekam kesehatan elektronik tersebut dan segala perubahanya dapat diketahui.

Berdasarkan artikel yang telah ditemukan, dapat diketahui bahwa tidak semua rekam medik elektronik dapat memfasilitasi adanya perubahan atau melakukan pencoretan tanpa menghilangkan data yang lama. Seperti pada Pada Klinik Medical *Check-Up* bahwa instalasi pada rekam medik elektronik memiliki kekurangan yaitu klinik belum mampu merekam data baru tanpa menghilangkan data yang lama [10]. Hal tersebut dapat dikatakan bahwa aspek integritas belum cukup baik, informasi dapat dikatakan dapat dipertanggungjawabkan jika informasi tersebut memiliki integritas. Salah satu hal yang menjadi kekhawatiran yakni sistem informasi klinik belum cukup mampu merekam data baru tanpa menghilangkan data lama. Sehingga, memang sangat dibutuhkan integritas dari *user* agar memastikan kegiatan *input* data berjalan dengan baik dan benar. Sama halnya dengan RSUD dr Moewardi yang menyebutkan bahwa di rumah sakit tersebut belum memfasilitasi perubahan informasi, pencoretan/penghapusan tidak dapat dilakukan dalam rekam medis elektronik [11].

Berbeda dengan penelitian sebelumnya, pada RSUD Ratu Zalecha Martapura bahwa perubahan yang bersifat besar harus mengkonfirmasi kepada bagian IT dan bagian IT yang akan melakukan perubahan dengan sepengetahuan semua pihak yang terlibat [8]. Sedangkan pada SIMKES yang ada belum mampu untuk dijadikan sebagai pedoman dalam pengambilan keputusan dalam sebuah pelayanan, hal ini dikarenakan belum adanya verifikasi data pada SIMKES dengan pelayanan yang sebenarnya terjadi [29]. Hal ini belum sesuai dengan integritas data yang berkaitan *dengan accuracy, consistency, dan completeness* dari data. Hal ini terkait dengan kualitas data yang bersangkutan dan dapat berpengaruh terhadap kualitas pelayanan kesehatan yang diberikan.

Hasil review dari artikel yang telah dibahas menunjukkan bahwa tidak semua fasilitas kesehatan dapat menjamin aspek *integrity* pada sistem informasinya. Hal tersebut dapat menimbulkan resiko perubahan informasi bahkan pemalsuan data asli milik pasien. Sehingga pemilik atau pengelola sistem informasi rekam medik elektronik perlu melakukan pengembangan terhadap sistem informasi yang ada dengan memaksimalkan metode atau cara yang digunakan sehingga data pasien yang tersimpan tidak dapat diubah kecuali oleh pemilik informasi. Saat ini informasi telah menjadi suatu kebutuhan yang penting bagi masyarakat. Kemampuan untuk mengakses dan menyediakan informasi secara tepat dan akurat menjadi penting bagi suatu organisasi fasilitas kesehatan. Pentingnya informasi menyebabkan perlu dilakukan pengamanan terhadap informasi untuk menjaga keabsahan dan nilai yang dimiliki oleh informasi tersebut, agar tidak disalahgunakan oleh pihak lain yang tidak bertanggung jawab.

3.4 Analisis Aspek *Authentication* pada Penerapan Rekam Medik Elektronik di fasilitas kesehatan

Authentication adalah aspek keamanan yang berhubungan dengan akses terhadap informasi. Atau cara untuk menyatakan keabsahan dari seorang pengguna. Dalam hal ini pengguna harus menunjukkan bukti bahwa memang dia adalah pengguna yang sah. Sebanyak 12 literatur yang diteliti menyebutkan beberapa teknik yang dapat menjamin aspek *authentication* yaitu tanda tangan elektronik dan penggunaan *id users.*

Penerapan tanda tangan elektronik /adanya *user id* dan *password* dokter untuk mengakses pada sistem rekam medik elektronik keaslian informasi rekam medis elektronik dapat dipertanggung jawabkan (bahwa yang mengisi adalah benar-benar dokter yang memeriksa pasien). Catatan rekam medis harus dibubuhi nama, waktu, dan tanda tangan petugas yang memberikan pelayanan atau tindakan [4]. Pasal yang sama ayat (3) menyebutkan "apabila dalam pencatan rekam medis menggunakan teknologi informasi elektronik, kewajiban membubuhi tanda tangan dapat diganti dengan menggunakan nomor identitas pribadi (*PIN*)"

Sebagian besar artikel yang telah dibahas menjelaskan bahwa aspek *authentication* dapat diterapkan dengan adanya id untuk masing-masing *user*/pengguna. Pencatatan rekam medis yang menggunakan teknologi informasi elektronik, tetap harus membubuhi tanda tangan yang dapat diganti dengan menggunakan *Personal Identification Numbe*r (PIN) [5].Penggunaan *id* pengguna dinilai belum maksimal menjaga keamanan data pada RME dikarenakan *id* pengguna dapat dengan mudah diketahui dan pihak lain ataupun apabila id pengguna telah diganti akan tetapi pengguna yang bersangkutan lupa id yang baru maka akan menyulitkan dalam penginputan data.

Tanda tangan digital memiliki berbagai manfaat bagi individu maupun perusahaan sehingga penggunaan tanda tangan digital ini sangat penting untuk fasilitas pelayanan kesehatan seperti rumah sakit. Selain itu, tanda tangan digital memiliki sistem enkripsi yang aman, dapat menghindari risiko pemalsuan tanda tangan atau penyalahgunaan pihak yang tidak bertanggungjawab, ramah lingkungan, efisien dan dilindungi oleh penjamin. Tanda tangan digital pada rekam medis elektronik adalah untuk memberikan autentifikasi dan penjagaan atas privasi terhadap isi atau data medis tiap-tiap pasien yang dibubuhkan pada akhir dokumen sebelum dokumen tersebut disimpan dalam sebuah sistem informasi manajemen rumah sakit (SIMRS-*EMR*) secara elektronik. Tanda tangan digital menjadi kunci utama dari aspek ini. Tanpa tanda tangan digital, rekam medis elektronik akan menjadi lubang dari privasi data pasien yang seharusnya dilindungi sepenuhnya oleh pihak rumah sakit. Selain itu, ketiadaan tanda tangan digital menyebabkan rekam medis menjadi tidak berlaku dan tidak mempunyai jaminan yang sah di depan hukum, sehingga hal ini dapat mengancam status sosial, psikologis dan jiwa pasien yang ditangani oleh profesi pemberi asuhan.

Sistem keamanan dengan menggunakan PIN (*Personal Identification Number*), kartu identitas (*Identification Card*) dan kata sandi (*password*) belum dapat sepenuhnya menjamin sistem keamanan yang mampu melindungi data pribadi seseorang. Faktanya, cara tersebut dapat dengan mudah diketahui oleh orang lain atau dibobol dengan sistem canggih sehingga dapat menimbulkan kerugian. Sistem keamanan saat ini dikembangkan menggunakan teknologi yang dapat melindungi sistem keamanan dengan baik yaitu menggunakan teknologi Biometrik. Dalam perkembangannya, sistem keamanan biometrik semakin diminati karena dianggap lebih akurat dan tak bisa dipalsukan, seperti menggunakan pemindaian pengenal, telapak tangan, jari, retina, atau pengenalan wajah [23].

Terdapat beberapa prinsip kerja pada sistem keamanan biometrik, diantaranya yaitu akurasi dari implementasi biometrik dimana pada teknologi biometrik akan memberikan peningkatan yang signifikan dalam akurasi pengidentifikasian identitas seseorang. Kemudian prinsip kerja yang selanjutnya yaitu metode pembuktian keaslian, pengiriman informasi dalam pelayanan, privasi masyarakat dan faktor eksternal. Dan salah satu teknologi biometrik yang sedang populer saat ini adalah sistem pengenalan wajah (*face recognition*).

3.5 Analisis Aspek *Availability* Pada Penerapan Rekam Medik Elektronik Di Fasiitas Kesehatan

Aspek *availability* merupakan aspek yang menekankan bahwa informasi ketika dihubungkan oleh pihak-pihak yang terkait tersedia secara cepat. Sebanyak 6 artikel yang diteliti menyebutkan bahwa tidak semua fasilitas kesehatan mampu menjamin aspek availability dalam rekam medik elektroniknya. Rekam medis harus selalu tersedia secara cepat dan dapat menampilkan kembali data yang telah tersimpan sebelumnya. Untuk rekam kesehatan ekektronik juga harus mempunyai sifat ketersediaan.

Beberapa artikel menunjukkan bahwa ketersediaan data rekam medis elektronik bisa di akses secara cepat didalam sistem sehingga mempermudah tenaga kesehatan mencari data yang dibutuhkan atau data yang baru saja di-*input*. Penyelengaraan sistem elektronik wajib mengoperasikan sistem elektronik yang memenuhi persyaratan minimum dapat menampilkan kembali informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang diterapkan dalam peraturan perundang-undangan [30]. Penelitian yang dilakukan di Klinik *Medical Check Up* menunjukkan bahwa keamanan sistem informasi klinik dilihat dari aspek kerahasiaan belum cukup baik [10]. Hal ini disebabkan oleh rumah sakit belum melakukan audit internal maupun eksternal terhadap sistem informasi klinik MP sehingga belum terdapat pengakuan *ISO 27001*. Sama halnya dengan penelitian yang menunjukkan bahwa aspek *availability* pada RSUD dr. Moewardi belum terlaksana secara maksimal, dikarenakan dalam pelaksanaannya masih membutuhkan dokumen rekam medis kertas khususnya bagi pasien rawat jalan yang direkomendasikan untuk rawat inap dan membutuhkan pemeriksaan penunjang. dan membutuhkan pemeriksaan penunjang (belum adanya fasilitas pencitraan *Picture Archieving and Communication Servive* (*PACS*) [11].

Aspek *availability* juga dapat dibuktikan dengan hubungan dengan organisasi lain khususnya BPJS yaitu mempermudah proses klaim pasien BPJS. Hubungan dengan pasien pun semakin meningkat dengan layanan barunya pendaftaran lewat aplikasi dan bisa *booking* pelayanan jauh-jauh hari, pelayanan pasien menjadi lebih baik diantaranya waktu tunggu pasien dipoliklinik membaik, efisien waktu pelayanan, dan juga pelayanan obat. Dengan diterapkannya aspek tersebut dapat memudahkan tidak hanya dokter yang merawat, tetapi juga pasien sebagai penerima layanan. Aspek *availability* berkaitan dengan apakah sebuah data tersedia saat dibutuhkan atau diperlukan. Apabila sebuah data atau informasi terlalu ketat pengamanannya akan menyulitkan dalam akses data tersebut. Disamping itu akses yang lambat juga menghambat terpenuhnya aspek *availability*. Berdasarkan hasil review dari artikel yang telah ditemukan,

beberapa artikel yang telah membahas mengenai penerapan aspek tersebut membuktikan bahwa tidak semua fasilitas kesehatan dapat menerapkan aspek *availability* dalam menjamin keamanan data pasien pada rekam medik. Penyelengaraan sistem elektronik wajib mengoperasikan sistem yang memenuhi persyaratan dapat menampilkan kembali Informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang diterapkan dalam peraturan perundang-undangan [31].

3.6 Aspek *Acces Control* pada Penerapan Rekam Medik Elektronik di fasilitas kesehatan

Aspek *acces control* adalah aspek yang berhubungan dengan pengaturan akses pengguna kepada suatu sistem informasi. Proses *access control* digunakan untuk memastikan bahwa hanya orang-orang yang berwenang dan punya alasan yang absah, terkait dengan pengoperasian sistem informasi kesehatan. *Access control* dapat mengatur siapa-siapa saja yang berhak untuk mengakses infomasi atau siapa-siapa saja yang tidak berhak mengakses informasi. Hal ini dimaksudkan agar keamanan data pasien didalamnya dapat terjamin. Sebanyak 9 artikel menyebutkan bahwa telah diterapkannya pengaturan *access control* pada sistem informasi pada rumah sakit, puskesmas atau klinik. *Access control* sering kali dilakukan dengan menggunakan kombinasi *user id* dan *password* atau dengan menggunakan mekanisme lainnya.

Penelitian yang dilakukan di Puskesmas Pleret menjelaskan bahwa hak akses diberikan kepada semua petugas Puskesmas dan orang luar dengan menggunakan *password* dan tanpa ada pengawasan dari petugas [32]. Hal ini dapat menimbulkan resiko kebocoran informasi data pasien oleh pihak yang tidak bertanggung jawab. *Access control* seharusnya diterapkan dengan melakukan batasan hak akses antara staff rekam medis dan kepala rekam medis berbeda. Misalnya di bagian pendaftaran, hanya di instal sistem pendaftaran saja dan hanya bisa mengakses sistem pendaftaran saja. Untuk kepala rekam medis, komputer di ruang kepala rekam medis di install aplikasi pendaftaran dan *assembling*, karena kepala rekam medis berwenang untuk mengetahui dan mengecek aktifitas yang di lakukan oleh semua petugas rekam medis, sedangkan sistem *Filing* hanya menjadi hak akses untuk petugas *filing* saja.

Rekam medik elektronik hanya dapat diakses oleh pengguna tertentu. Jika ada pasien yang membutuhkan resume medis maka pasien harus mengisi surat permintaan terlebih dahulu. Prosedur ini melindungi rekam medis elektronik dari petugas yang tidak berwenang. Hak akses catatan pengguna dapat diberikan secara terperinci kepada perusahan atas seijin pengguna [33]. Penyelenggara sistem elektronik wajib melaksanakan prinsip pelindungan data pribadi dalam melakukan pemrosesan data pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, adil, dengan sepengetahuan dan persetujuan dari pemilik data pribadi [31].

Penelitian yang dilakukan di Rumah Sakit Avicean Medika Martapura menunjukkan bahwa pada rumah sakit tersebut belum ada aturan secara resmi yang menerapkan siapa saja yang dapat mengakses rekam medis elektronik tersebut, tetapi sudah terdapat draf-draf yang berhak dan berwenang dalam hak akses rekam medis elektronik namun belum disahkan secara resmi [8]. Hal tersebut belum sesuai dengan peraturan bahwa persyaratan tata kelola sistem elektronik adalah terdapat mekanisme yang berkelanjutan untuk menjaga kebaruan dan kejelasan prosedur pedoman pelaksanaan serta adanya kelembagaan dan kelengkapan personel pendukung bagi pengoperasian sistem elektronik sebagaimana mestinya [31].

Pada dasarnya, fasilitas kesehatan telah menerapkan aspek *access control* pada rekam medik elektroniknya dengan melakukan pembatasan hak akses, namun masih ada beberapa fasilitas kesehatan yang belum maksimal dalam menerapkan pembatasan hak akses. Hal tersebut dapat dapat menimbulkan resiko kebocoran karena terbukanya data oleh pihak yang tidak memiliki wewenang dalam mengakses informasi tersebut. Sehingga pengelola sistem harus dapat memastikan bahwa pengguna yang masuk pada sistem adalah pengguna yang sah atau yang berhak menggunakannya.

3.7 Aspek *Non-Repudiation* dalam Penerapan Rekam Medik Elektronik di fasilitas kesehatan

Aspek *non repudiation* adalah aspek yang dapat menjaga seseorang untuk menyangkal bahwa telah melakukan transaksi atau pengoperasian pada sistem informasi pada sistem rumah sakit, klinik atau puskesmas [10]. Sebanyak 6 artikel yang telah ditemukan menyebutkan bahwa telah menerapkan aspek ini pada sistem informasi kesehatannya.

Transaksi atau perubahan terhadap suatu informasi data akan terlihat dan terlacak langsung pada bagian IT rumah sakit [8]. Setiap ada yang menginput ataupun menghapus data informasi kedalam rekam medis elekteronik akan langsung terdapat pemberitahuan di *log file* pada bagian IT. Penyelenggara Sistem Elektronik wajib menyediakan rekam jejak audit terhadap seluruh kegiatan penyelenggaraan Sistem

Elektronik. Rekam jejak audit sebagaimana dimaksud digunakan untuk keperluan pengawasan, penegakan hukum, penyelesaian sengketa, verifikasi, pengujian, dan pemeriksaan lainnya [31].

Berbeda dengan penelitian sebelumnya bahwa proses transaksi hanya dapat diketahui oleh tim IT, bahwa aspek *non repudiation* ditunjukkan dengan terfasilitasinya cara melihat riwayat data yang telah dilakukan pengisian, apabila terdapat perubahan data maka riwayat data tersimpan dan tidak bisa dihilangkan [16], [34]. Sedangkan RSUD dr. Moewardi menyebutkan bahwa aspek *non repudiation* belum dilaksanakan secara maksimal, akibatnya sistem tidak dapat mengidentifikasi pengguna yang telah melakukan perubahan informasi pasien pada rekam medik elektronik [11]. Hal tersebut dapat menimbulkan pengguna atau seseorang dapat menyangkal telah melakukan transaksi pada sistem elektronik tersebut. Sehingga dapat dikatakan bahwa penyelenggaraan pengamanan data dalam sistem elektronik masih belum maksimal.

Setiap tindakan yang dilakukan dalam sebuah sistem yang aman harus diawasi (*logged*), ini dapat berarti penggunaan alat untuk melakukan pengecekan sistem berfungsi sebagaimana seharusnya. Fitur riwayat transaksi juga tidak dapat dipisahkan dari bagian keamanan sistem yang dimana bila terjadi sebuah penyusupan atau serangan lain akan sangat membantu proses investigasi. Pemilihan jenis metode transmisi juga mempunyai peranan penting didalam masalah keamanan. Setiap informasi rahasia tidak boleh di transmisikan tanpa menggunakan enkripsi yang bagus, sehingga setiap orang dapat menyadap komunikasi yang terkirim. Aspek ini sangat penting dalam hal transaksi elektronik. Penggunaan *digital signature* dan teknologi kriptografi secara umum dapat menjaga aspek ini. Akan tetapi hal ini masih harus didukung oleh hukum sehingga status dari *digital signature* itu jelas legal.

4. KESIMPULAN

4.1 Kesimpulan

Berdasarkan hasil penelitian dari 20 artikel yang telah *direview* dapat diketahui keamanan informasi data pasien yang ditinjau dari aspek keamanan informasi *(Privacy, Integrity, Authentication, Availability, Access Control, Non-Repudiation)* yaitu:

1. Aspek *privacy* pada penerapan rekam medik elektronik di fasilitas kesehatan dilakukan dengan beberapa cara yaitu penggunaan *username* dan *password* bagi masing-masing pengguna, *automatic log off,* pemblokiran akses dengan teknologi jaringan, dan teknologi enkripsi data.
2. Aspek *integrity* pada penerapan rekam medik elektronik di fasilitas kesehatan dilakukan dengan perubahan atau penghapusan data oleh administrator.
3. Aspek *authentication* pada penerapan rekam medik elektronik di fasilitas kesehatan diterapkan dengan adanya tanda tangan elektronik, penggunaan PIN, penggunaan sidik jari, serta tanda file *signature*.
4. Aspek *availability* pada penerapan rekam medik elektronik di fasilitas kesehatan dibuktikan dengan dapat terhubungnya sistem informasi kesehatan dengan perusahaan lain khususnya BPJS kesehatan, serta menggunakan proses *back up* data guna mengantisipasi peretasan data pasien.
5. Aspek *acces control* pada penerapan rekam medik elektronik di fasilitas kesehatan diterapkan dengan dilakukannya pembatasan hak akses dengan penggunaan *user id* & *password* bagi masing-masing pengguna, serta kebijakan pengaksesan data harus dengan seijin pemilik data atau pasien.
6. Aspek *non repudiation* pada penerapan rekam medik elektronik di fasilitas kesehatan diterapkan dengan adanya *log file* untuk melihat proses transaksi serta penggunaan kunci publik dan pribadi.

4.2 Saran

1. Pengguna sistem sebaiknya meningkatkan kesadaran terkait keamanan data dan melakukan penggantian *password* secara berkala dalam menjamin aspek *privacy*.
2. Pengelola sistem sebaiknya mengembangkan metode yang digunakan untuk memantau perubahan data dalam menjamin aspek *integrity.*
3. Pengelola sistem sebaiknya sebaiknya mengembangkan teknik-teknik yang digunakan seperti *one-way hashes* sampai *smart cards* yang menggunakan teknik-teknik *strong encryption* dalam menjamin aspek *authentication.*
4. Pengelola sistem sebaiknya mengembangkan teknik yang digunakan seperti sistem *backup* dan menyediakan *disaster recovery center (DRC)* yang dilengkapi dengan panduan untuk melakukan pemulihan *(disaster recovery plan)* dalam menjamin aspek *availability.*
5. Fasilitas kesehatan sebaiknya melakukan pengadaan kebijakan terkait pembatasan hak akses untuk meminimalisir pengoprasian atau transaksi pada sistem oleh pengguna yang bukan memiliki hak akses guna menjamin aspek *acces control*

6. Pengelola sistem sebaiknya mengembangkan sistem untuk lebih *auditable* atau dapat diperiksa dengan mudah untuk menjamin aspek *non-repudiation.*

UCAPAN TERIMA KASIH

Ucapan terima kasih peneliti sampaikan kepada dosen pembimbing dan dosen penguji saya yang telah membimbing saya sampai menyelesaikan penelitian ini.

REFERENSI

[1] Permenkes RI No 43 tahun 2019, "Permenkes No 43 tahun 2019 tentang Pusat kesehatan masyarakat," no. 2, pp. 5–10, 2019.
[2] N. A. Samandari, W. C. S, and A. H. Rahim, "Kekuatan Pembuktian Rekam Medis Konvensional Dan Elektronik," *SOEPRA*, vol. 2, no. 2, p. 154, 2017, doi: 10.24167/shk.v2i2.818.
[3] "undang-undang-nomor-29-tahun-2004-tentang-praktik-kedokteran.pdf." .
[4] 29 UU RI Nomor, "UU No. 29 Tahun 2004 Tentang Praktik Kedokteran," *Aturan Prakt. Kedokt.*, pp. 157–180, 2004.
[5] PERMENKES RI No 269/MENKES/PER/III/2008, "permenkes ri 269/MENKES/PER/III/2008," *Permenkes Ri No 269/Menkes/Per/Iii/2008*, vol. 2008. p. 7, 2008.
[6] N. F. Octarina, M. B. N. Wajdi, and, "Tinjauan terhadap UU ITE untuk Penerapan Rekam Medis Berbasis Online pada Penduduk Muslim di Indonesia," *At-Tahdzib* 2017, [Online]. Available: http://ejournal.kopertais4.or.id/mataraman/index.php/tahdzib/article/view/3253.
[7] Permenkes RI No 11 tahun 2008 "Permenkes no 11 tahun 2008 tentang informasi dan transaksi elektronik,". 69–73, 2008.
[8] N. Rahmadiliyani and F. Faizal, "Kerahasiaan Rekam Medis Di Rumah Sakit Aveciena Medika Martapura [Online]. Available: https://www.jmiki.aptirmik.or.id/index.php/jmiki/article/view/189.
[9] I. Tambang, "Cadas! jokowi cabut 2.078 izin tambang," 2022.
[10] D. R. A. Tiorentap and H. Hosizah, "Aspek Keamanan Informasi dalam Penerapan Rekam Medis Elektronik di Klinik Medical Check-Up MP," *ISBN 978-623-6566-34-3*, 2020, [Online]. Available: https://prosiding.esaunggul.ac.id/index.php/FHIR/article/view/71.
[11] N. D. Pratiwi and A. A. Mudayana, "Identifikasi Kelengkapan Rekam Medis Pasien Hyperplasia Of Prostate Di Rumah Sakit Pku Muhammadiyah Bantul," *Med. Respati J. Ilm. Kesehat.*, vol. 14, no. 3, p. 233, 2019, doi: 10.35842/mr.v14i3.204.
[12] D. R. A. Tiorentap and H. Hosizah, "Aspek Keamanan Informasi dalam Penerapan Rekam Medis Elektronik di Klinik Medical Check-Up MP,". *ISBN 978-623-6566-34-3*, 2020, [Online]. Available: https://prosiding.esaunggul.ac.id/index.php/FHIR/article/view/71.
[13] S. W. Nugraheni, "Aspek Hukum Rekam Medis Elektronik di RSUD Dr Moewardi Legal Aspects of Electronic Medical Record in RSUD Dr Moewardi ada dua , yaitu aspek finansial dan aspek legal dan security . Secara umum rekam medis," vol. 1, pp. 92–97, 2018.
[14] A. R. Pahlevi, E. S. Wardhana, and E. D. Agustin, "Electronic Medical Record At Rsigm Sultan Agung Semarang Reviewed From The Completeness And The Safety Format System," *J. Medali*, 2021,http://lppm-unissula.com/jurnal.unissula.ac.id/index.php/medali/article/view/16892.
[15] H. N. Saputra, "Surya Medika Analisis Keamanan Data Sistem Informasi," vol. 12, no. 2, pp. 96–105, 2017.
[16] N. Innab, "Availability, Accessibility, Privacy and Safety Issues Facing Electronic Medical Records,". vol. 7, no. 1, pp. 01–10, 2018, doi: 10.5121/ijsptm.2018.7101.
[17] M. Amin, W. Setyonugroho, and N. Hidayah, "Implementasi Rekam Medik Elektronik: Sebuah Studi Kualitatif," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 1, pp. 430–442, 2021, doi: 10.35957/jatisi.v8i1.557.
[18] M. E. Fitriyani and R. M. D. Rohmadi, "Tinjauan Fitur Keamanan Data Pada Pilar Unit Rekam Medis Sistem Informasi Manajemen Rumah Sakit (Simrs)" *Rekam Medis*, 2016, [Online]. Available: https://ejurnal.stikesmhk.ac.id/index.php/rm/article/view/591.
[19] P. Vimalachandran, H. Wang, and Y. Zhang, "Securing electronic medical record and electronic health record systems through an improved access control," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9085, pp. 17–30, 2015, doi: 10.1007/978-3-319-19156-0_3.

[20] D. U. Waisantoro, R. M. D. Rohmadi, and S. Mulyono, "Tinjauan Penerapan Otentifikasi Keamanan Sistem Informasi Managemen Rumah Sakit Umum Daerah Surakarta," *Rekam Medis*, 2014, [Online]. Available: https://ejurnal.stikesmhk.ac.id/index.php/rm/article/viewFile/294/268.
[21] N. Rahmadiliyani and F. Faizal, "Kerahasiaan Rekam Medis Di Rumah Sakit Aveciena Medika Martapura," *J. Manaj. Inf. Kesehat. Indones.*, vol. 6, no. 2, p. 69, 2018, doi: 10.33560/.v6i2.189.
[22] K. P. Andriole, "Security of electronic medical information and patient privacy: What you need to know," *J. Am. Coll. Radiol.*, vol. 11, no. 12, pp. 1212–1216, 2014, doi: 10.1016/j.jacr.2014.09.011.
[23] L. B. Harman, C. A. Flite, and K. Bond, "State Of The Art And Science Electronic Health Records: Privacy, Confidentiality, and Security," *Am. Med. Assoc. J. Ethics*, vol. 14, no. 9, pp. 712–719, 2012, [Online]. Available: www.virtualmentor.org712.
[24] E. Sari and S. Mulyono, "Tinjauan Fitur Keamanan Data Pasien Pada Sistem Informasi Manajemen Puskesmas Di Puskesmas Polokarto Kabupaten Sukoharjo," *Rekam Medis*, 2016, [Online]. Available: https://ejurnal.stikesmhk.ac.id/index.php/rm/article/view/588.
[25] "No Title," 2016.
[26] W. Vera and S. Putri, "Tinjauan Keamanan Data Rekam Medis Pasien Pada Program Studi D-Iii Perekam Dan Informasi Kesehatan Stikes Ngudia Husada Madura Tahun 2021," 2021.
[27] A. D. APL, - Rohmadi, and S. Mulyono, "Tinjauan Fitur Keamanan Data Pasien Pada Sistem Informasi Rawat Jalan Berbasis Komputerisasi Di Balai Besar Kesehatan Paru Masyarakat Surakarta Tahun 2013," *J. Manaj. Inf. Kesehat. Indones.*, vol. 1, no. 2, pp. 79–88, 2013, doi: 10.33560/.v1i2.55.
[28] O. M. Enaizan, N. H. Alwi, and N. J. Zaizi, "Privacy and Security Concern for Electronic Medical Record Acceptance and Use: State of the Art Article Info," *J. Adv. Sci. Eng. Res.*, vol. 7, no. 2, pp. 23–34, 2017.
[29] A. D. APL, - Rohmadi, and S. Mulyono, "Tinjauan Fitur Keamanan Data Pasien Pada Sistem Informasi Rawat Jalan Berbasis Komputerisasi Di Balai Besar Kesehatan Paru Masyarakat Surakarta Tahun 2013," *J. Manaj. Inf. Kesehat. Indones.*, vol. 1, no. 2, 2013, doi: 10.33560/.v1i2.55.
[30] P. Pemerintah *et al.*, "Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik," no. 2, 2016.
[31] T. Saputra and E. Kurniadi, "Sistem Informasi Rekam Medis Pasien Rawat Jalan Di Uptd Puskesmas Kuningan Berbasis Web," *NUANSA Inform.*, vol. 13, no. 2, p. 19, 2019, doi: 10.25134/nuansa.v13i2.1949.
[32] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egypt. Informatics J.*, vol. 22, no. 2, pp. 177–183, 2021, doi: 10.1016/j.eij.2020.07.003.
[33] A. R. Pahlevi *et al.*, "RSIGM Agung Semarang belum digunakan secara menyeluruh . Rekam medis elektronik dalam tahap perkembangan," vol. 3, no. September, pp. 20–28, 2021.