Procedia of Engineering and Life Science Vol. 9 2025
Proceedings of the 2025 Annual Meeting of APTIRMIKI
Strengthening the Competence of PMIK Candidates to Create Excellent Human Resources in the Digital Health Era

Evaluation of Core Security Principles in Electronic Medical Records

Evaluasi Prinsip Keamanan Dasar dalam Catatan Medis Elektronik

Hendra Rohman[1], Alfia Salsabilah Lauma[2], Sukma Dian Pambudi[3], Indra Narendra[4]

Politeknik Kesehatan Bhakti Setya Indonesia, Yogyakarta, Indonesia
Email: hendrarohman@mail.ugm.ac.id

Abstract *— EMR access in one of health centers in Yogyakarta City are given to all health service officers using username and password. In registration, there are 2 username while 5 registration officers use them. This can pose a risk of data and patient information leakage. This study aims to evaluate 6 aspects of information security in EMR in health center. This type of research is qualitative. The population is 51 EMR users and sample is 7 users. Privacy, on access rights, login process to EMR uses a username and password, automatic log out feature does not yet exist. Integrity, on accuracy data and timeliness in filling out forms, accuracy of data is accurate but timeliness in filling is sometimes less timely due to system downtime in form of network problems and power outages, edit and delete features are already available but not all users can use these features. Authentication, on electronic signatures has not been implemented but manual signatures that are carried out can still guarantee authentication from users, on application of signatures to guarantee validity of users made using electronic certification provider services has not been implemented. Availability, data transfer to the health office is not done at health center, as health office can retrieve the necessary data using a superadmin user. Access control, access are set using a username and password, in accordance with user access settings, duties, and authorities. Non-repudiation, a history of access and edits is maintained for users using EMR.*
Keywords*— System Evaluation, Data Security, Electronic Medical Records*

Abstrak—Hak akses RME di salah satu puskesmas Kota Yogyakarta diberikan kepada semua petugas Faskes menggunakan *username* dan *password*. Di bagian pendaftaran terdapat 2 *username* namun yang menggunakan 5 petugas pendaftaran. Hal ini dapat menimbulkan resiko adanya kebocoran data dan informasi pasien. Tujuannya mengevaluasi 6 aspek keamanan informasi pada RME di puskesmas. Jenis penelitian kualitatif. Populasi adalah 51 pengguna RME dan sampel yang diambil 7 pengguna. Aspek *privacy*, pada hak akses, proses *login* ke RME menggunakan *username* dan *password*, pada fitur *log out* otomatis belum ada. Aspek *integrity*, pada keakuratan data dan ketepatan waktu dalam mengisi formulir, keakuratan data sudah akurat tetapi ketepatan waktu dalam mengisi kadang kurang tepat waktu karena terjadi *downtime system* berupa masalah jaringan dan pemadaman listrik, pada fitur edit dan hapus sudah ada namun tidak semua pengguna bisa menggunakan fitur tersebut. Aspek *authentication*, pada tanda tangan elektronik belum menerapkan namun tanda tangan manual yang dilakukan tetap bisa menjamin otentikasi dari pengguna, pada penerapan tanda tangan untuk menjamin keabsahan pengguna yang dibuat dengan menggunakan jasa penyelenggara sertifikasi elektronik belum diterapkan. Aspek *availability*, pada aspek ketersediaan pengiriman data ke Dinkes tidak dilakukan di puskesmas karena dari pihak Dinkes bisa mengambil data yang diperlukan dengan menggunakan *user superadmin*. Aspek *access control*, pengaturan hak akses dengan *username* dan *password*, sesuai dengan pengaturan hak akses pengguna serta tugas dan wewenangnya. Aspek *non-repudiation*, sudah terdapat riwayat bagi pengguna yang menggunakan RME terkait apa saja yang diakses dan diedit.
Kata Kunci— Evaluasi Sistem, Keamanan Data, Rekam Medis Elektronik

I. PENDAHULUAN

Undang-undang Republik Indonesia Nomor 27 Tahun 2022 tentang perlindungan data pribadi (PDP) mengatur tentang keamanan dan kerahasiaan rekam medis elektronik (RME) diwajibkan untuk mematuhi ketentuannya, termasuk penggunaan RME. Beberapa hal yang di atur dalam UU PDP terkait keamanan dan kerahasiaan RME yaitu pimpinan Fasyankes bertanggung jawab atas keamanan RME, seluruh pihak yang memiliki akses terhadap data RME wajib menjaga kerahasiaannya, subjek data pribadi berhak atas akuntabilitas pihak yang meminta data pribadi, dan setiap Fasyankes bertanggung jawab untuk menjaga kerahasiaan dan privasi data pasien. RME bisa diakses dengan komputer dari suatu jaringan dengan tujuan utama menyediakan atau meningkatkan perawatan serta pelayanan kesehatan yang efisien dan terpadu (Khasanah, 2020).

Di salah satu puskesmas Kota Yogyakarta sudah menggunakan RME sejak tahun 2023. Lokasi awal implementasi RME dilakukan di puskesmas pembantu pada bulan Februari 2023. Hak akses RME diberikan kepada semua petugas pelayanan kesehatan puskesmas dengan menggunakan *username* dan *password*. Di puskesmas terdapat 53 hak akses pengguna namun yang menggunakan RME 51 petugas pelayanan kesehatan. Di bagian pendaftaran terdapat 2 *user* sedangkan yang menggunakan 5

petugas pendaftaran Hal ini dapat menimbulkan resiko adanya kebocoran data dan informasi pasien. Tujuan penelitian ini mengevaluasi aspek *privacy, integrity, authentication, availability, access control, non-repudiation* pada RME di puskesmas.

II. METODE

Jenis penelitian kualitatif dengan rancangan studi kasus. Populasi adalah semua pengguna RME yaitu 51 pengguna yang terdiri dari pendaftaran, kasir, dokter, dokter gigi, dokter internship, perawat, farmasi, laboratorium, gizi, bidan, psikologi, dan surveilans. Sampel adalah 7 pengguna yaitu perekam medis, perawat, dokter, ahli teknologi (IT), dokter gigi, dan gizi. Pengumpulan data melalui observasi, wawancara, dan dokumentasi. Data diolah secara deskriptif dalam bentuk narasi.

III. HASIL DAN PEMBAHASAN

A. HASIL

1. Evaluasi Aspek *Privacy* RME

a. Hak Akses

Aspek kerahasiaan atau *privacy* merupakan usaha menjaga informasi pasien dari pihak-pihak yang tidak memiliki hak untuk mengakses informasi atau data pasien. Data rekam medis yang disimpan dan didistribusikan secara elektronik rentan disalah gunakan sehingga dapat merugikan pasien. Kerahasiaan merupakan jaminan keamanan data dan informasi dari gangguan pihak internal maupun eksternal yang tidak memiliki hak akses, sehingga data dan informasi yang ada dalam RME terlindungi pengunaan dan penyebarannya. Berikut tampilan kolom pengisian *username* dan *password*:

Gambar 1. Tampilan kolom pengisian *username* dan *password*

Proses untuk *login* ke sistem RME menggunakan *username* dan *password*. *Username* dan *password* dalam RME digunakan untuk membuktikan bahwa pengguna memiliki wewenang untuk memakai dan masuk ke dalam sistem untuk menghindari percobaan pengaksesan oleh pengguna yang tidak memiliki wewenang. Menjaga keamanan sistem dengan *password* masih memiliki beberapa kelemahan. Terutama pada pengguna memiliki *password* yang mudah dan tidak dilakukan *reset password*.

b. Fitur *Log Out* Otomatis

Fitur *log out* otomatis dalam RME, bertujuan untuk meningkatkan keamanan dan mencegah penyalahgunaan data pasien oleh orang yang tidak berwenang. Sistem akan secara otomatis mengeluarkan pengguna dari RME jika tidak ada aktivittas dalam jangka waktu tertentu. Di puskesmas belum terdapat fitur *log out* otomatis. Fitur *log out* otomatis sangat penting untuk mencegah orang yang tidak berhak mengakses sistem, jika *user* keluar meninggalkan sistem dalam keadaan terbuka, fitur ini juga melindungi data pasien dari akses yang tidak sah.

2. Evaluasi Aspek *Integrity* RME

a. Keakuratan Data dan Ketepatan Waktu dalam Mengisi Formulir

Integritas adalah aspek keamanan yang menjamin tidak adanya pengubahan data tanpa seizin pihak yang berwewenang, menjaga keakuratan dan keutuhan informasi. Integritas memastikan data tidak diubah oleh pengguna atau proses yang tidak sah dan menjaga konsistensi data secara internal maupun eksternal. Integritas merupakan jaminan terhadap keakuratan data dan

informasi yang ada dalam RME, dan perubahan terhadap data hanya boleh dilakukan oleh orang yang diberi hak akses untuk mengubah data pasien dalam sistem RME.

Keakuratan data dan ketepatan waktu dalam mengisi formulir identitas pasien di puskesmas sudah berjalan cukup baik. Keakuratan data sudah akurat tetapi untuk ketepatan waktu dalam mengisi kadang kurang tepat waktu karna terjadinya *downtime system*. *Downtime system* berupa masalah jaringan dan pemadaman listrik. Cara penanganan di puskesmas sudah sesuai dengan SOP yang berlaku. Terdapat 2 SOP tentang penulisan atau pengisian dan ketepatan dari isi rekam medis elektronik yaitu SOP penulisan rekam medis elektronik dan SOP penilaian kelengkapan dan ketepatan isi rekam medis.

Keakuratan data dan ketepatan waktu data pasien dapat dinyatakan akurat, hanya saja pada ketepatan waktu kadang masih kurang dikarenakan adanya *downtime system* yang memperlambat proses pelayanan kesehatan. Terdapat SOP pengisian rekam medis saat terjadi kendala listrik atau jaringan di puskesmas yaitu SOP pengisian rekam medis saat kendala listrik/jaringan.

b. Fitur Edit dan Hapus

Pada RME sudah terdapat fitur edit dan hapus sebagai bentuk pengeditan data. Namun tidak semua pengguna dapat menggunakan fitur tersebut.


Log Anamnesis

No	Tgl	Keluhan - RPS - Nyeri	RPD - RPK - Alergi	Add	Edit	Delete
1	11-06-2025 08:00:00	KEL: PUNGGUNG BAGIAN BAWAH TERASA MUNCUL SAKIT DAN NYERI, RIWAYAT TERBENTUR (+) RPS: KONTROL TENSI KEMARIN TENSI TINGGI 140N NYR: –	RPD: – RPK: HT ALGI TIDAK ADA	11-06-2025 08:18:45.558461	--	--

Gambar 2. Tampilan fitur edit dan hapus

Sistem RME terdapat fitur edit dan hapus tetapi tidak semua pengguna bisa menggunakan fitur tersebut. Hal ini sejalan dengan kebijakan Permenkes No. 24 tahun 2022 tentang rekam medis yang menjelaskan data rekam medis tidak boleh dihapus dalam rangka perlindungan data pribadi.

Aspek keamanan data pasien dalam implementasi RME di puskesmas cukup baik karena di dalamnya sudah terdapat fitur edit yang hanya digunakan oleh petugas sesuai dengan hak aksesnya berdasarkan tugas, wewenang, dan tanggung jawabnya dalam pelayanan di puskesmas. Aspek keamanan di puskesmas sudah sesuai dengan tugas dan wewenangnya masing-masing.

3. Evaluasi Aspek *Authentication* RME

a. Penerapan Tanda Tangan Elektronik (TTE)

Autentikasi merupakan aspek keamanan data pasien yang berkaitan dengan akses informasi atau bagaimana sistem menyatakan keabsahan untuk pengguna dapat mengakses data di dalam sistem. Metode yang dapat digunakan untuk autentikasi pengguna dapat menggunakan kata sandi, nomor identitas, biometrik dan lain sebagainya. Tidak hanya itu, penggunaan *username* dan *password* juga termasuk dalam menjaga keamanan data pasien, cara lain yang dapat digunakan untuk menjaga keamanan data pasien dari aspek autentikasi adalah dengan adanya penerapan TTE. TTE digunakan sebagai alat verifikasi dan autentikasi atas RME dan identitas penanda tangan.

Di puskesmas belum menerapkan TTE. Tetapi tanda tangan manual yang dilakukan di puskesmas tetap bisa menjamin otentikasi dari pengguna. Penggunaan TTE di puskesmas masih menggunakan tanda tangan manual. Dimana petugas akan memberikan berkas atau formulir yang akan ditanda tangani oleh dokter.

b. Penerapan TTE dalam Menjamin Keabsahan Pengguna

Tanda tangan elektronik adalah tanda tangan yang terdiri atas informasi elektronik yang diletakkan, terasosiasi atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi. Penanda tangan adalah subjek hukum yang terasosiasikan atau terkait dengan tanda tangan elektronik. Menurut pasal 11 UU ITE, tanda tangan elektronik memiliki

kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan. Penerapan TTE di puskesmas tentang pentingnya penerapan TTE dalam menjamin keabsahan pengguna terdapat beberapa petugas yang setuju dan tidak.

TTE terdapat beberapa persyaratan yang memiliki kekuatan hukum merupakan tanda tangan yang dibuat dengan menggunakan jasa penyelenggara sertifikasi elektronik, dan hal tersebut belum diterapkan di puskesmas. Autentikasi dapat dinyatakan bahwa aspek keamanan data pasien dalam implementasi TTE di RME belum diterapkan namun penggunaan tanda tangan manual juga tetap bisa menjamin keabsahan dokumen dan masih bisa dijadikan sebagai bukti otentik yang sah.

4. Evaluasi Aspek *Availability* RME

Ketersediaan atau *availability* merupakan aspek yang menjamin data akan tersedia saat dibutuhkan kapanpun dan dimanapun bagi *user* yang memiliki hak akses. Penyimpanan RME harus menjamin keamanan, keutuhan, kerahasiaan, dan ketersediaan data RME. RME sebagai alat komunikasi diwajibkan untuk selalu tersedia secara cepat serta dapat menampilkan kembali data yang telah tersimpan sebelumnya.

Di puskesmas, aspek ketersediaan RME pengiriman data yang dibutuhkan oleh pihak dinas kesehatan sudah tidak dilakukan di puskesmas. Dinas kesehatan bisa langsung mengambil data yang dibutuhkan dengan menggunakan user *superadmin* yang dimiliki oleh dinas kesehatan tanpa harus pergi ke puskesmas.

Pengiriman data di puskesmas sudah tidak melakukan pengiriman data karena bisa langsung diakses oleh pihak dinas kesehatan dengan menggunakan *user* yang disebut *superadmin*. Ketersediaan merupakan jaminan data dan informasi yang ada dalam RME dapat di akses dan digunakan oleh orang yang telah memiliki hak akses yang ditetapkan oleh pimpinan Fasyankes. Terdapat SOP *back-up* data di puskesmas yaitu SOP *back-up* data SIMPUS.

Aspek ketersediaan pengiriman data ke dinas kesehatan tidak dilakukan di puskesmas karena dari pihak dinas kesehatan bisa mengambil data yang diperlukan dengan menggunakan *user superadmin*.

5. Evaluasi Aspek *Access Control* RME

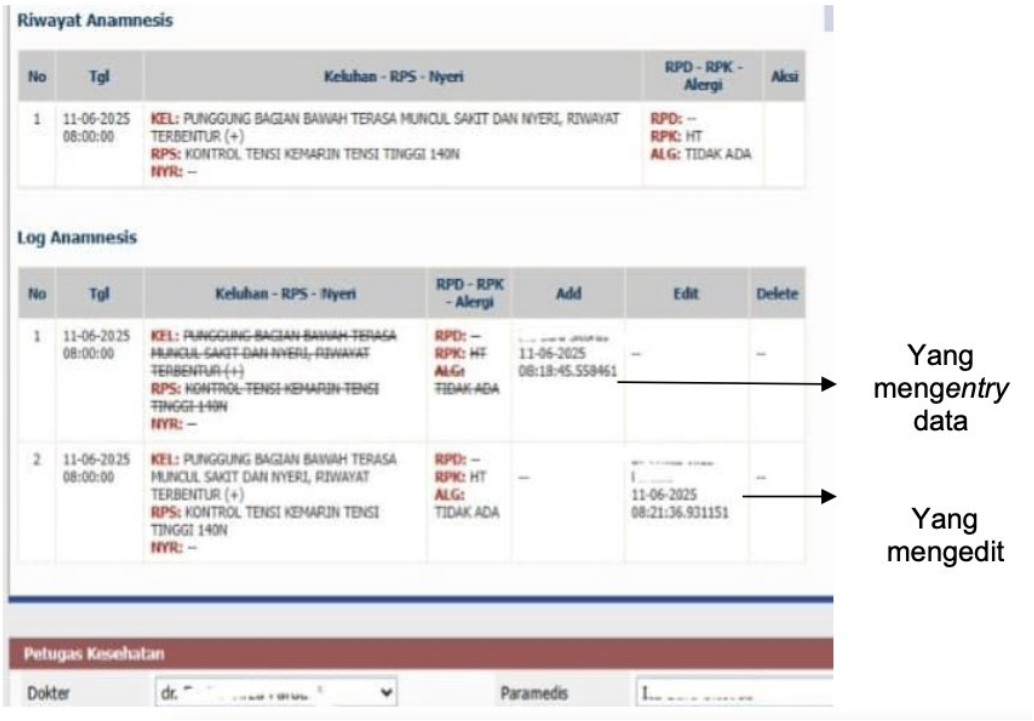
Accsess control merupakan aspek yang berkaitan dengan bagaimana pengaturan akses pengguna terhadap sistem informasi, proses ini dilakukan untuk memastikan hanya petugas yang memiliki hak akses yang dapat menggunakan sistem informasi kesehatan. Dengan adanya *access control* dapat menjaga keamanan data pasien dengan cara menggunakan *username* dan *password* untuk mengatur pengguna EMR serta membatasi hak akses *user*. Hasil hak akses dari setiap pengguna berbeda sesuai dengan tugas, wewenang, dan tanggung jawab.

Pengaturan hak akses yang digunakan di puskesmas dengan penerapan *username* dan *password*. Hal ini sesuai dengan pengaturan hak akses pengguna *health information system* (HIS) sesuai dengan tugas dan wewenangnya masing-masing. Berdasarkan peraturan yang bisa mengakses RME diatur dalam kebijakan pimpinan Fasyankes, dengan memperhatikan prinsip keamanan data dan informasi. Prinsip keamanan data dan informasi menjadi fokus utama dalam mengatur hak akses RME, yang bertujuan untuk meningkatkan mutu pelayanan kesehataan, memberikan kepastian hukum, menjamin keamanan data dan kerahasiaan data, serta mewujudkan penyelenggaraan dan pengelolaan rekam medis tercapai.

Terdapat SOP RME di puskesmas yaitu SOP rekam medis elektronik. Akses kontrol dan pengaturan akses RME sudah sesuai dengan peraturan yang sudah ditetapkan.

6. Evaluasi Aspek *Non-Repudiation* RME

Non-repudiation merupakan bagaimana sistem dapat merekam jejak perubahan data yang dilakukan oleh pengguna. Menurut peraturan pemerintah nomor 71 tahun 2019 tentang penyelenggaraan sistem dan transaksi elektronik menjelaskan bahwa wajib menyediakan rekam jejak audit terhadap seluruh kegiatan penyelenggaraan sistem elektronik yang digunakan untuk keperluan pengawasan, penegakkan hukum, penyelesaian sengketa, verifikasi, pengajuan, dan pemeriksaan lainnya.



Gambar 3. Tampilan nama yang mengentry dan mengedit data

Di puskesmas sudah terdapat *history* bagi pengguna yang menggunakan RME. Di puskesmas dalam sistem RME sudah terdapat riwayat pengguna RME terkait apa saja yang diakses dan diedit. Hal ini sejalan dengan penelitian yang dilakukan menjelaskan bahwa perubahan data riwayat rekam medis pasien harus dapat diketahui dengan jelas, apabila terdapat perubahan data maka riwayat data tersimpan dan tidak bisa dihilangkan dalam penulisan RME.

B. PEMBAHASAN

1. Evaluasi Aspek *Privacy* RME

a. Hak Akses RME

Aspek keamanan RME tentang hak akses data sangat penting untuk melindungi privasi pasien dan memastikan integritas data. Hak akses harus dibatasi hanya pada pengguna yang berwenang, dengan menggunakan *username* dan *password* sebagai bentuk otentikasi. Data rekam medis harus dienkripsi saat disimpan dan ditransmisikan untuk melindungi privasi dan mencegah akses yang tidak sah. Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang rekam medis pasal 30 disebutkan bahwa dalam rangka keamanan dan perlindungan data RME, pimpinan Fasyankes memberikan hak akses kepada tenaga kesehatan di Fasyankes.

Pada halaman *login* terdapat *username* dan *password*. *User* melakukan *login* dengan mengisikan *username* dan *password*. Fungsi dari halaman *login* yaitu untuk masuk ke halaman menu utama sistem informasi (Rohman dan Prasetyo, 2023).

Penggunaan hak akses di puskesmas sudah menggunakan *username* dan *password* yang digunakan untuk membuktikan bahwa pengguna memiliki wewenang untuk memakai dan masuk ke dalam sistem RME dan menghindari adanya percobaan pengaksesan oleh pengguna yang tidak memiliki wewenang. Penggunaan hak akses di puskesmas sudah sesuai dengan peraturan Menteri Kesehatan nomor 24 tahun 2022, dimana hak akses RME hanya petugas yang memiliki hak dan wewenang untuk mengakses RME.

b. Fitur *Log Out*

Otomatis fitur *log out* otomatis merupakan aspek penting dalam menjaga keamanan dan privasi data pasien. RME menyimpan data sensitif pasien, sehingga keamanan dan privasi data tersebut menjadi sangat penting. Fitur *log out* otomatis membantu mencegah akses yang tidak sah ke data tersebut jika pengguna meninggalkan sistem tanpa menutupnya secara manual.

Fitur ini meminimalkan risiko data pasien dibaca oleh orang yang tidak berwenang jika pengguna lupa untuk *log out*. Setelah periode inaktivitas waktu 5 menit, sistem secara otomatis keluar dari akun pengguna, sehingga mencegah potensi akses yang tidak sah (Tiorentap *et.al,* 2020). Aspek *privacy* dibuktikan dengan bentuk melakukan *log out* otomatis sistem RME di Fasyankes jika dalam kurun waktu 5 menit tidak terjadi aktivitas yang dilakukan oleh *user* (Sofia *et.al.,* 2022). Penggunaan fitur *log out* otomatis berfungsi sebagai salah satu bentuk pertahanan dalam penyalahgunaan hak akses *username*. Di puskesmas penggunaan fitur *log out* otomatis belum ada karena dikhawatirkan nanti petugas akan merasa kesusahan dan akan menghambat pelayanan pasien.

Penggunaan fitur *log out* otomatis di puskesmas belum ada, hal ini belum sesuai dengan penelitian Tiorentap *et al.,* (2020) dan Sofia *et al.,* (2022) karena fitur *log out* otomatis sangat penting untuk mencegah orang yang tidak berhak mengakses sistem.

2. Evaluasi Aspek *Integrity* RME

a. Keakuratan Data dan Ketepatan Waktu dalam Mengisi Formulir

Keakuratan data RME sangat penting dalam pelayanan kesehatan karena data yang akurat membantu dalam diagnosis, perencanaan perawatan, dan pengambilan keputusan medis yang efektif. Dengan sistem RME, kesalahan manusia dalam pencatatan data dapat diminimalisir, meningkatkan keakuratan dan integritas informasi pasien. Ketepatan data rekam medis juga sangat penting untuk memastikan akurasi informasi kesehatan pasien, yang berdampak pada kualitas pelayanan dan pengambilan keputusan medis. RME yang akurat dan tepat meminimalkan kesalahan dan potensi duplikasi data, serta memudahkan pertukaran informasi antar fasilitas kesehatan. Peraturan Menteri Kementrian Kesehatan Republik Indonesia Nomor 24 tahun 2022 pasal 29 ayat 3 tentang integritas merupakan jaminan terhadap keakuratan data dan informasi yang ada dalam RME dan perubahan data yang bisa dilakukan oleh orang yang diberi hak akses untuk mengubah.

Di puskesmas, keakuratan data dan ketepatan waktu dalam mengisi formulir identitas, asesmen maupun diagnosa pasien sudah berjalan dengan baik karena untuk pasien dengan KTP Kota Yogyakarta itu bisa langsung *link* ke data Dukcapil jadi otomatis datanya sudah sesuai. Sedangkan, untuk pasien KTP luar Yogyakarta itu harus diisi manual sesuai dengan KTP pasien dan dilengkapi dengan domisili pasien. Tetapi, untuk ketepatan waktu dalam mengisinya kadang kurang tepat waktu karna sering terjadinya *downtime system*. Keakuratan data pasien dalam mengisi formulir identitas pasien, asesmen, dan diagnosa pasien itu sudah akurat dan sesuai dengan Permenkes, hanya saja pada ketepatan waktu masih terjadinya *downtime system* yang membuat terhambatnya proses pengisian formulir.

b. Fitur Edit dan Hapus

Menurut Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 tahun 2022 pasal 30 tentang perubahan atau perbaikan data yang hanya dapat dilakukan oleh tenaga kesehatan pemberi pelayanan kesehatan. Fitur edit dalam RME diperbolehkan dengan batasan waktu dan pihak yang berwenang, sedangkan fitur hapus tidak diperbolehkan. Perbaikan data hanya dapat dilakukan oleh tenaga kesehatan yang memberikan pelayanan dan petugas administrasi, termasuk perekam medis dan informasi kesehatan. Batas waktu perbaikan data paling lama 2x24 jam sejak data di*input* perubahan data juga harus dicatat dengan jelas. Fitur hapus tidak diperbolehkan karena data harus tetap tersedia untuk kepentingan audit analisis dan lain-lain. Jika terjadi kesalahan dalam penulisan maka dilakukan perubahan atau perbaikan bukan menghapus data. Dalam hal kesalahan data adminstratif diketahui melebihi tenggat waktu 2x24 jam, maka perbaikan dilakukan setelah mendapat persetujuan dari perekam medis informasi dan kesehatan atau pimpinan Fasyankes.

Di puskesmas, RME sudah terdapat fitur edit dan hapus sebagai bentuk pengubahan data. Namun tidak semua pengguna dapat menggunakan fitur tersebut. Hanya pengguna yang mengentry pelayanan dan bagian *user admin* yang bisa melakukan pengubahan data. Pengeditan atau pengubahan data di puskesmas tidak bisa melewati 2x24 jam, tetapi bagi yang memiliki *user admin* masih bisa mengubah dengan proteksi disertai dengan alasan yang tepat. Hal ini sudah sesuai dengan Permenkes 2022, karena sudah terdapat fitur edit dan hapus yang hanya bisa digunakan oleh petugas yang memiliki wewenang dan tanggung jawab dalam pelayanan di puskesmas.

3. Evaluasi Aspek *Authentication* RME

a. Penerapan Tanda Tangan Elektronik (TTE)

Tanda tangan elektronik merupakan solusi efektif dan efisien untuk mendukung digitalisasi berbagai proses, mulai dari transaksi bisnis hingga penanda tanganan dokumen. Dengan pemahaman yang tepat tentang jenis dan legalitasnya, penggunaan

tanda tangan elektronik (TTE) dapat memberikan manfaat yang signifikan bagi individu. Di Indonesia, penggunaan TTE diatur dalam Undang-Undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik (UU ITE), yang kemudian diubah dengan UU nomor 19 tahun 2016. UU ITE mengakui TTE tersertifikasi sebagai bukti sah dan setara dengan tanda tangan basah, asalkan memenuhi persyaratan.

Menurut Permenkes RI Nomor 24 Tahun 2022 pada pasal 31, dalam rangka keamanan dan perlindungan data, penyelenggaraan RME di Fasyankes dapat dilengkapi dengan adanya tanda tangan elektronik. Tanda tangan ini digunakan sebagai alat verifikasi dan autentikasi dalam pencatatan dan pendokumentasian informasi klinis.

Tanda tangan manual (tanda tangan basah) dalam rekam medis merujuk pada tanda tangan yang ditulis tangan di atas dokumen rekam medis fisik. Tanda tangan ini berfungsi sebagai verifikasi bahwa informasi dalam rekam medis telah dicatat dengan benar oleh tenaga kesehatan.

TTE di puskesmas belum ada, masih mempertahankan tanda tangan manual atau tanda tangan asli. Ketika ada formulir yang membutuhkan tanda tangan petugas kesehatan maka, petugas akan menanda tangani formulir tersebut dengan penggunakan tanda tangan asli.

Di puskesmas belum menggunakan dan menerapkan TTE. Tetapi penggunaan tanda tangan manual yang dilakukan di puskesmas masih bisa dijadikan bukti otentikasi dan sah dari setiap petugas, dan bisa menjadi jaminan keabsahan dokumen.

b. Penerapan TTE dalam Menjamin Keabsahan Pengguna

Setiap penyelenggara sistem elektronik harus menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawa terhadap beroperasinya sistem elektronik sebagaimana mestinya jaminan keamanan dan kehandalan sistem elektronik dalam pelayanan kesehatan. Semua sistem elektronik wajib untuk menggunakan tanda tangan digital dalam setiap dokumen elektronik yang digunakan untuk setiap dokumen elektronik yang digunakan untuk transaksi, baik untuk transaksi pertukaran dokumen maupun transaksi lainnya.

Tindakan pengesahan atau persetujuan dokumen yang sah dan diakui adalah berupa tanda tangan digital, bukan tanda tangan basah hasil pemindaian yang disematkan di dokumen atau dengan menandatangani langsung dokumen menggunakan fitur *draw* di *microsoft* atau *PDF reader*. Cara tersebut tidak dapat menjamin keabsahan dan keauntetikan dokumen elektronik karena cara ini mudah dilakukan pemalsuan serta sulit mengetahui adanya perubahan terhadap informasi elektronik dan waktu penanda tanganan (Yuniati dan Sidiq, 2020). Standar Prosedur Operasional (SPO) yang diterbitkan, dijadikan sebagai pedoman dalam pelaksanaan menjaga kerahasiaan rekam medis maupun proses pelaksanaannya. Ketersediaan formulir persetujuan secara tertulis sebagai bentuk menjaga kerahasiaan berkas rekam medis (Rohman, 2020).

Menurut Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 pada pasal 31, dalam rangka keamanan dan perlindungan data, penyelenggaraan RME di Fasyankes dapat dilengkapi dengan TTE. TTE dalam RME berfungsi untuk autentikasi dan verifikasi identitas penandatanganan serta keutuhan dan keabsahan informasi elektronik. TTE ini juga memegang peranan penting dalam lingkungan kesehatan untuk mengotorisasi dan memverifikasi informasi medis, serta memberikan legitimasi hukum pada dokumen digital.

Di puskesmas terdapat beberapa pengguna yang setuju dan tidak setuju dengan adanya TTE karena takutnya akan disalahgunakan oleh orang yang tidak berwenang dan tidak bertanggung jawab. Kecuali, TTE dibuat dengan menjalankan ketentuan-ketentuan yang sesuai dengan peraturan undang-undang. Di puskesmas sedang proses pengajuan untuk adanya TTE. Penerapan TTE bisa dikatakan sah dan aman kalau TTE dibuat dengan mentaati dan menjalankan sesuai dengan ketentuan-ketentuan tertentu.

4. Evaluasi Aspek *Availability* RME

Aspek *availability* dalam keamanan RME mengacu pada ketersediaan dan aksesibilitas data RME secara tepat waktu dan andal. Ketersediaan merupakan jaminan data dan informasi yang ada dalam RME dapat di akses dan digunakan oleh orang yang telah memiliki hak akses dan digunakan oleh orang yang telah memiliki hak akses yang ditetapkan oleh pimpinan Fasyankes (Permenkes, 2022). Aspek *availability* merupakan aspek yang menekankan bahwa informasi ketika dihubungkan oleh pihak-pihak yang terkait secara cepat. Ketersediaan data RME bisa di akses secara cepat di dalam sistem sehingga mempermudah tenaga kesehatan untuk mencari data yang dibutuhkan atau data yang baru saja di*input* (Sofia, *et al.,* 2022).

Di puskesmas untuk ketersediaan pengiriman data sudah tidak dilakukan karena pihak dari puskesmas bisa langsung mengakses dan mengambil data apa saja yang dibutuhkan dengan menggunakan *user superadmin*. Di puskesmas sudah sesuai

dimana pengiriman dan keamanan data pasien sudah terjamin dengan pengiriman data dilakukan langsung oleh *user superadmin* yaitu orang yang bekerja di dinas kesehatan dan bisa hanya bisa dengan dilakukan di lingkungan puskesmas dengan menggunakan jaringan puskesmas atau jaringan pemerintah kota (Pemkot).

5. Evaluasi Aspek *Access Control* RME

Aspek *access 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, terkait dengan pengoperasian sistem informasi kesehatan, juga keamanan data pasien dapat terjamin. *Access control* dapat mengatur siapa saja yang berhak untuk mengakses informasi atau siapa saja yang tidak berhak mengakses informasi (Sofia, *et al.,* 2022). Sistem *access control* bertujuan untuk menjaga kerahasiaan data pasien dan memastikan penggunaan data rekam medis hanya dilakukan oleh pihak yang berwenang. RME hanya dapat diakses dan digunakan oleh orang yang memiliki hak akses sesuai yang ditetapkan oleh pimpinan Fasyankes. Sistem rekam medis juga harus menjaga keamanan dan kerahasiaan data serta memastikan data tidak berubah tanpa adanya izin (Permenkes, 2022). Evaluasi secara keseluruhan menimbulkan dampak positif karena kualitas sistem yang digunakan dapat menghasilkan *output* informasi yang baik, lengkap dan sesuai kebutuhan (Rohman *et al.,* 2022).

Di puskesmas, aspek *access control* dilakukan dengan menggunakan *username* dan *password* yang diberikan kepada setiap petugas dan unit pelayanan kesehatan. Masing-masing pengguna *username* dan *password* memiliki tugas dan tanggung jawab masing-masing. Di puskesmas untuk akses kontrol *username* dan *password* sudah sesuai, dimana setiap unit dan petugas pelayanan kesehatan memiliki masing-masing *username* dan *password* dengan tugas dan tanggung jawab masing-masing.

6. Evaluasi Aspek *Non-Repudiation* RME

Aspek *non-repudiation* adalah aspek yang dapat menjaga seseorang untuk menyakal bahwa telah melakukan transaksi atau pengoperasian pada sistem informasi rumah sakit, klinik, atau puskesmas. Penyelenggaraan sistem elektronik wajib menyediakan rekam jejak audit terhadap seluruh kegiatan penyelenggaraan sistem elektronik. Rekam jejak audit yang dimaksud digunakan untuk keperluan pengawasan, penegakan hukum, penyelesaian sengketa, verifikasi, pengujian, dan pemeriksaan lainnya (Sofia, *et al.,* 2022). Setiap transaksi atau perubahan pada RME, seperti penambahan catatan medis, pengeditan data, atau akses oleh petugas, akan tercatat dalam *log file*. *Log file* ini mencakup informasi seperti siapa yang melakukan perubahan, kapan perubahan terjadi, dan apa yang telah diubah (Permenkes, 2022).

Di puskesmas, fitur riwayat jejak audit biasanya dilakukan jika terdapat perubahan atau penghapusan data, pada sistem pengubahan data tetap bakal ke rekam siapa yang merubah dan apa yang diubah. Tetapi hak akses untuk mengubah dan menghapus hanya bisa dilakukan oleh *admin* dan rekam medis. Di puskesmas sudah sesuai, dimana pengubahan bisa dilakukan dengan tetap merekam apa aja yang diubah dan siapa yang mengubah.

III. SIMPULAN

Evaluasi aspek *privacy*, pada hak akses, proses *login* ke RME menggunakan *username* dan *password*, pada fitur *log out* otomatis belum ada. Evaluasi aspek *integrity*, pada keakuratan data dan ketepatan waktu dalam mengisi formulir, keakuratan data sudah akurat tetapi ketepatan waktu dalam mengisi kadang kurang tepat waktu karena terjadi *downtime system* berupa masalah jaringan dan pemadaman listrik, pada fitur edit dan hapus sudah ada namun tidak semua pengguna bisa menggunakan fitur tersebut.

Evaluasi aspek *authentication*, pada TTE belum diterapkan, TTE dalam proses pengajuan namun tanda tangan manual yang dilakukan tetap bisa menjamin otentikasi dari pengguna, pada penerapan TTE dalam menjamin keabsahan pengguna yang dibuat dengan menggunakan jasa penyelenggara sertifikasi elektronik belum diterapkan. Evaluasi aspek *availability*, pada aspek ketersediaan pengiriman data ke dinas kesehatan tidak dilakukan di puskesmas karena dari pihak dinas kesehatan bisa mengambil data yang diperlukan dengan menggunakan *user superadmin*.

Evaluasi aspek *access control*, pengaturan hak akses dengan *username* dan *password*, sesuai dengan pengaturan hak akses pengguna setiap unit dan petugas pelayanan kesehatan serta tugas dan wewenangnya. Evaluasi aspek *non-repudiation*, sudah terdapat riwayat bagi pengguna yang menggunakan RME terkait siapa dan apa saja yang diakses serta diedit.

Pada fitur *log out* otomatis, sebaiknya pihak dari puskesmas mengajukan dan melakukan penerapan fitur *log out* otomatis untuk menjaga adanya akses dari pihak yang tidak berwenang dan menjamin keamanan data pasien. Keadaan *downtime system*

yang sering terjadi, sebaiknya dilakukan pemeliharaan rutin pada perangkat keras maupun perangkat lunak. Pada penerapan TTE, sebaiknya pihak dari puskesmas memastikan legalitas dan kepatuhan regulasi TTE agar bisa menjamin keabsahan dokumennya.

REFERENSI

Kementerian Kesehatan Republik Indonesia. (2022). Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022. Jakarta: Kementerian Kesehatan RI.

Khasanah, M. (2020). Tantangan Penerapan Rekam Medis Elektronik Untuk Instansi Kesehatan. Jurnal Sainstech, 7(2), 50–53.

Rohman, H. (2020). Tinjauan Pelepasan Informasi Medis Dalam Menjamin Aspek Hukum Kerahasiaan Rekam Medis di Rumah Sakit Umum Rajawali Citra. JCOMENT (Journal of Community Empowerment), 1(3), 85–95.

Rohman, H., Ismiyati, N., Irianto, I. D. K., Nurrochman, A., & Saputra, R. P. (2022). Pendampingan Kegiatan Evaluasi Sistem Informasi Posyandu Lansia Bougenvile Padukuhan Tegalwaras, Sariharjo, Kapanewon Ngaglik, Sleman, Yogyakarta. In Prosiding COSECANT: Community Service and Engagement Seminar (Vol. 2, No. 2). Yogyakarta: Universitas Ahmad Dahlan.

Rohman, H., & Prasetyo, R. A. (2023, July). Perancangan Sistem Informasi Manajemen Klinik Berbasis Web di Klinik Mitra Husada Nglipar. In Prosiding Seminar Informasi Kesehatan Nasional (pp. 1–11). Yogyakarta: Universitas Ahmad Dahlan.

Sofia, S., Ardianto, E. T., Muna, N., & Sabran, S. (2022). Analisis Aspek Keamanan Informasi Data Pasien pada Penerapan RME di Fasilitas Kesehatan. Jurnal Rekam Medik & Manajemen Informasi Kesehatan, 1(2), 94–103. https://doi.org/10.47134/rmik.v1i2.29

Tiorentap, D. R. A., & Hosizah, H. (2020). Aspek Keamanan Informasi dalam Penerapan Rekam Medis Elektronik di Klinik Medical Check Up MP. 4th Proceeding Perspektif Implementasi FHIR. Jakarta: Universitas Indonesia.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik. (2016). Jakarta: Sekretariat Negara Republik Indonesia.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, Termasuk Data Dalam Rekam Medis. (2022). Jakarta: Sekretariat Negara Republik Indonesia.

Yuniati, T., & Sidiq, M. F. (2020). Literature Review: Legalisasi Dokumen Elektronik Menggunakan Tanda Tangan Digital Sebagai Alternatif Pengesahan Dokumen di Masa Pandemi. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 4(6), 1058–1069.