RAMMIK : Jurnal Rekam Medik dan Manajemen Informasi Kesehatan
Vol. 3, No. 2, Oktober 2024, hlm. 18 - 30
EISSN: 2829-4777
URL : https://rammik.pubmedia.id/index.php/rmik

ANALISIS ASPEK KEAMANAN DATA PASIEN DALAM IMPLEMENTASI REKAM MEDIS ELEKTRONIK DI RUMAH SAKIT X

Efri Tri Ardianto[1], Sabran[2*], Lensa Nurjanah[3],

[1,2,3]Program Studi Manajemen Informasi Kesehatan, Jurusan Kesehatan, Politeknik Negeri Jember
efritriardianto@polije.ac.id ,sabran@polije.ac.id,lensanurjanah@gmail.com

Keywords:

Data Security Aspects,
Electronic Medical Record,

ABSTRACT

Computer-based health records are electronic patient records to support users in complete & accurate access. The benefits of electronic medical records (RME) are very important, but there are several threats that are of particular concern that could have a detrimental impact. Health data theft has become a serious problem. Based on observations & interviews, problems were found from the security aspect at Hospital The research used a qualitative approach, collecting data through interviews, observation, documentation with research subjects of 7 respondents. Data was analyzed by data reduction, data presentation & conclusions. The results show that security from the confidentiality aspect is logging in using username & password but not changing it regularly and there is no SOP. From the integrity aspect, there is a data editing feature for users according to their main duties and functions. Editing large amounts of data cannot be done directly but must comply with the SOP. The Authentication aspect has implemented a certified electronic signature to guarantee validity. The availability aspect of RME can only be accessed within the hospital environment with VPN so it is easy to access. The access control aspect to limit user access rights is implemented by username & password. The non-denial aspect provides a history of users accessing patient data.

Kata Kunci

Aspek Keamanan Data,
Rekam Medis Elektronik,

ABSTRAK

Rekam kesehatan berbasis komputer merupakan rekaman pasien secara elektronik untuk mendukung pengguna mengakses secara lengkap & akurat. Manfaat rekam medis elektronik (RME) sangat penting tetapi terdapat beberapa ancaman yg menjadi perhatian khusus dpt berdampak merugikan. Pencurian data kesehatan mengalami peningkatan menjadi permasalahan serius. Berdasarkan observasi & wawancara ditemukan permasalahan dari aspek keamanan di Rumah Sakit X. Tujuan penelitian untuk menganalisis aspek keamanan data pasien dlm penerapan RME berdasarkan aspek kerahasiaan, integritas, autentikasi, ketersediaan, akses kontrol, nir-sangkal. Penelitian menggunakan pendekatan kualitatif, pengumpulan data melalui wawancara, observasi, dokumentasi dgn subjek penelitian 7 responden. Data dianalisis dg reduksi data, penyajian data & kesimpulan. hasil menunjukkan bahwa keamanan dari aspek kerahasiaan yaitu login menggunakan username & password namun belum melakukan penggantian secara berkala serta belum adanya SOP. Dari aspek integritas terdapat fitur edit data untuk pengguna sesuai tupoksi, edit data dlm jumlah besar tidak dapat dilakukan secara langsung namun harus sesuai SOP. Aspek Autentikasi sudah menerapakan tanda tangan elektronik bersertifikat menjamin keabsahan. aspek ketersediaan RME hanya ddt diakses dilingkungan rumah sakit dengan VPN sehingga mudah diakses. Aspek kontrol akses untuk membatasi hak akses pengguna diterapkan username & password. Aspek Nir-sangkal terdapat riwayat bagi pengguna yg mengakses data pasien.

Korespondensi Penulis:

Sabran,
Politeknik Negeri Jember,

Email: Sabran@polije.ac.id

1. PENDAHULUAN

Teknologi informasi dan komunikasi yang selanjutnya di singkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, pengelolaan dan penyampaian atau pemindahan informasi antar sarana atau media [1]. Kebutuhaan untuk menggunakan teknologi informasi saat ini diperlukan untuk mendukung kinerja sebuah organisasi, teknologi informasi telah menjadi kebutuhan bagi semua bidang salah satunya adalah dalam layanan kesehatan. Dengan penggunaan sistem informasi dalam layanan kesehatan dapat memberikan banyak manfaat yang sangat menguntungkan bagi penyedia layanan kesehatan, seperti meningkatkan kualitas pelayanan, mengurangi kesalahan medis, meningkatkan pembacaan ketersediaan fasilitas dan aksesibilitas infromasi [2]

Rumah sakit merupakan salah satu instistusi pelayanan kesehatan yang menyelenggarakan pelayanan kesehatan perorangan secara paripurna baik rawat inap, rawat jalan, dan gawat darurat tentunya berkewajiban untuk menyelenggarakan rekam medis elektronik yang dilakukan sejak pasien masuk sampai pasien pulang, Rekam medis elektronik adalah dokumen yang berisikan data identitas pasien, pemeriksaan, pengobatan, tindakan, dan pelayanan lain yang telah diberikan kepada pasien. dirujuk, atau meninggal. [3]. Menurut Institute Of Medicine (1999) rekam kesehatan berbasis komputer *(Comupter-based patient record*/CPR*)* merupakan rekaman pasien yang dikerjakan secara elektronik dan berada di dalam sistem yang dirancang secara khusus untuk mendukung pengguna dalam mengakses data pasien secara lengkap dan akurat, yaitu dengan memberikan tanda peringatan, waspada, dan sistem pendukung pengambil keputusan klinis [3].

Terlepas dari berbagai manfaat yang dapat dirasakan dari penggunaan sistem rekam medis elektronik dalam bidang kesehatan, tentunya terdapat beberapa ancaman yang harus menjadi perhatian khusus bagi instnasi penyedia pelayanan kesehatan. Dengan pesatnya penggunaan teknologi informasi saat ini, dibutuhkan tata kelola teknologi informasi untuk menjaga keamanan informasi dan data [4]. Tren pencurian data yang terus meningkat menjadi permasalahan yang serius. Pencurian data kesehatan bukan hal baru di Indonesia. Pada tahun 2020 sebanyak 230 data pasien Covid-19 diketahui telah dicuri data kesehatannya, selain itu pada bulan januari tahun 2022 diduga telah terjadi pelanggaran data pada catatan pasien di beberapa rumah sakit di Indonesia sebesar 720 GB yang dijual di forum online [5]. *Ransomeware WannaCry* merupakan kasus kebocoran data terbesar didunia dimana dalam kasus ini sebanyak 150 negara menjadi korban dan mengakibatkan kelumpuhan sistem salah satunya adalah sistem informasi di Rumah Sakit Kanker Dharmais yang mengalami kelumpuhan sistem akibat dari hal tersebut dan menyebabkan penumpukan pasien [2].

Permenkes RI no 24 tahun 2022 tentang rekam medis telah mengatur tekait dengan keamanan rekam medis elektronik dimana rekam medis diselenggarakan secara elektronik dengan tujuan menjamin kemanan, kerahasiaan, keutuhan, dan ketersediaan data rekam medis yang harus memenuhi prinsip-prinsip keamanan data dan informasi yaitu kerahasiaan, integritas dan ketersediaan data [3]. Menurut *Health Insurance Portability and Acountability Act* (HIPAA) keamanan informasi haru memenuhi beberapa hal yaitu, 1) Memastikan kerahasiaan, integritas, dan ketersediaan semua informasi kesehatan serta melindungi dalam membuat, menerima, mempertahankan, atau mentransmisikan informasi kesehatan; 2) Melindungi dari ancaman dan bahaya yang diantisipasi secara wajar; 3) Melindungi dari pengguna atau penggungkapan informasi yang diantisipasi secara wajar berdasarkan perturan privasi; 4) Memastikan kepatuhan tenaga kerja [2].

Standar ISO/IEC 27001:2013 yaitu acuan standar sistem manajemen keamanan informasi yang dikeluarkan oleh "*International Organization for Standarization dan International Comission*" yang terdiri dari aspek keamanan informasi *confidently* (kerahasiaan), *availability* (ketersediaan), dan *integrity* (integritas). ISO/IEC 27001:2013 memberikan kerangka pembangunan, penerapan, pengoperasian, pemantauan, peminjaman dan peningkatan Sistem Manajemen Keamanan Informasi (SMKI) [4]. [6]menjelaskan bahwa prinsip keamanan mencakup *privacy, confidently, integrity, avaibility, nonrepudiation, authentication dan authorization*. Menururt Sabarguna (2008) dalam Nugraheni dan

Nurhayati (2018) aspek *privacy* atau *confidentiality* merupakan penjagaan informasi dari pihak-pihak yang tidak memiliki hak untuk mengakses informasi [7]. *Integrity* merupakan bagaimana tentang perubahan informasi. *Authentication* berkaitan dengan bagaimana akses terhadap informasi. *Availability* merupakan ketersediaan informasi bila dibutuhkan oleh pihak-pihak terkait. *Acces Control* merupakan cara pengaturan akses informasi dan *Nonrepudiation* merupakan transaksi informasi atau perubahan informasi.

Berdasarkan hasil wawancara dan observasi terkait rekam medis elektronik di Rumah Sakit X, diketahui terdapat beberapa permasalahan terkait keamanan rekam medis elektronik. Rekam medis elektronik akan terlog out secara otomatis apabila E-RM sudah tidak digunakan selama kurang lebih dari enam jam. Beberapa petugas tidak mematikan PC dan melogout rekam medis elektronik Ketika ditinggalkan dan tidak digunakan. Diketahui beberapa petugas belum melakukan penggantian username dan password secara berkala, hal ini penting dilakukan untuk menjaga kerahasiaan E-RM, apabila username dan password tersebut telah diketahui oleh pihak yang tidak berkepentingan. Kontrol akses dalam rekam medis elektronik dapat di implementasian melalui penggunaan *username dan password*. Selain itu diketahui belum adanya standar operasional prosedur (SOP) terakit penyelenggaran rekam medis elektronik atau SOP khusus terkait keamanan dan kerahasiaan data pasien dalam rekam medis elektornik. Standar operasional prosedure (SOP) mampu mengurangi dan menghindari kerentanan ancaman kemanan informasi serta menjadi pedoman dalam menjalankan aktivitas yang berkaitan dengan keamanan informasi [4].

2. METODE PENELITIAN

2.1 Jenis Penelitian

Jenis penelitian yang digunakan adalah penelitian kualitatif. Penelitian ini dilakukan di RS X.

2.2 Subyek Penelitian

Informan dalam penelitian ini sejumlah 7 petugas rumah sakit.

2.3 Pengumpulan Data

Pengumpulan data primer dilakukan melalui wawancara, observasi, dan dokumentasi.

2.4 Analisis Data

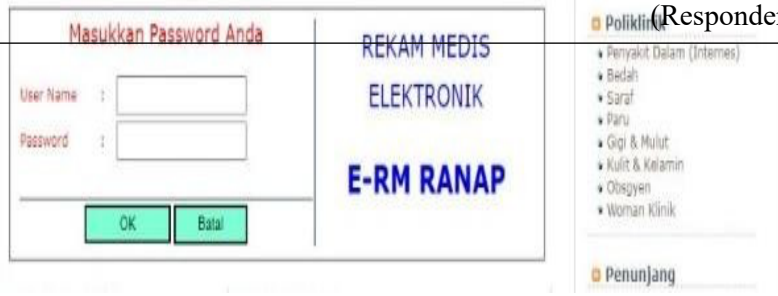
Analisis data dalam penelitian ini dilakukan dengan reduksi data, penyajian data, dan penarikan kesimpulan hasil penelitian. Uji keabsahan data dilakukan dengan triangulasi sumber dan triangulasi teknik.

3. HASIL DAN ANALISIS

3.1 Menganalisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik di Rumah Sakit X Berdasarkan Aspek Kerahasiaan (*Confidentiality*)

Aspek kerahasiaan atau confidentiality merupakan usaha menjaga informasi pasien dari pihak-pihak yang tidak memiliki hak untuk mengakses informasi tersebut. Data rekam medis yang disimpan dan didistribusikan secara elektronik rentan disalah gunakan sehingga dapat merugikan pasien [5]. Kerahasiaan merupakan jaminan keamanan data dan infromasi dari gangguan pihak internal maupun eksternal yang tidak memiliki hak akses, sehingga data dan infromasi yang ada dalam rekam medis elektronik terlindungi penggunaan dan penyebarannya [3]. Dari hasil penelitian yang dilakukan terkait dengan keamanan informasi dalam penerapan rekam medis elektronik di dapatkan hasil wawancara dengan responden sebagai berikut.

"dengan username dan password" (Responden 1, 2023)



Gambar 1. Menu Login ERM

Berdasarkan hasil wawancara dan observasi diketahui E-RM untuk login ke sistem E-RM menggunakan *username* dan *password*. Hal ini sesuai dengan penelitian yang dilakukan oleh [5] menjalaskan bahwa *username* dan *password* dalam E-RM 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 yang memiliki *password* yang mudah.

Dari hasil wawancara dengan responden diketahui bahwa penggunaan *password* di sistem E-RM belum menggunakan karater khusus. berikut adalah kutipan hasil wawancara dengan responden:

> "*Sudah ada, setiap session tertentu selama 30 menit apabila tidak digunakan, 30 menit karena untuk memudahkan dokter saat memberi pelayannan, karena jika cuma 5 menit dokter akan kerepotan jika harus login lagi"*
>
> (Responden 7, 2023)

> "*Belum"* (Responden 6, 2023)
>
> "*Ya"* (Responden 4, 2023)
>
> *"tergantung masing-masing petugas, himbauan sudah ada namun apabila di ubah terkadang bisa lupa"* (Responden 1, 2023)

> "*gak harus sulit"* (Responden 3, 2023)
>
> "*alphabetik"* (Responden 4, 2023)
>
> "*diharapkan angka dan huruf"* (Responden 1, 2023)

Dari beberapa pernyataan responden tersebut, sesuai dengan hasil wawancara dengan petugas bagian IT yaiut sebagai berikut:

> "*sebisa mungkin karakter khusus, walapun dalam pelaksanaannya kadang banyak yang mengeluhkan merekan lupa, semakin sulit password yang dibuat semakin tinggi potensi lupanya"*
>
> (Responden 7, 2023)

Melakukan penggantian *username* dan *password* secara berkala untuk menghindari apabila username dan password tersebut telah diketahui oleh pihak yang tidak berkepentingan. Berdasarkan hasil wawancara berikut adalah hasil yang diperoleh:

Pernyataan dari responden tersebut sesuai dengan penjelasan dari pihak bagian IT.Berikut adalah hasil wawancara dengan petugas bagian IT.

> "*harusnya sudah namun parkteknya sulit, kembali ke masing-masing personal, karena kesibukan terkadang kalo diganti sering lupa"*
>
> (Responden 7, 2023)

Berdasarkan dari hasil wawancara dengan seluruh responden diketahui dari tujuh responden 6 menyatakan belum melakukan penggantian *username* dan *password* secara berkala dan satu responden menyatakan iya dalam penggantian *username* dan *password* secara berkala. Penelitian yang dilakukan oleh [8] mengganti *password* secara berkala untuk menghindari jika kata sandi telah diketahui oleh pihak yang tidak berkepentingan. selain dengan username dan password dapat pula menggunakan teknik fitur *automatic logout* untuk menjamin kerahasiaan. Berikut adalah kutipan hasil wawancara dengan responden:

"*sudah ada"* (Responden 2, 2023)
"*Belum"* (Responden 5, 2023)

Responden menyatakan sudah ada fitur *automatic logout* dan satu responden menyatakan belum ada fitur *automatic logout*. Berdasarkan hasil wawancara dengan pihak IT diperoleh informasi bahwa sudah ada fitur *automatic logout*. Hal ini sejalan dengan penelitian yang dilakukan oleh [2] menjelaskan bahwa bentuk pertahanan adalah dengan sistem *automatic logout*, jika tidak terjadi aktivitas selama kurun waktu 5 (lima) menit, maka dengan otomatis akan melakukan logout . Berikut adalah pernyataan dari responden:

"*Sudah ada, setiap session tertentu selama 30 menit apabila tidak digunakan, 30 menit karena untuk memudahkan dokter saat memberi pelayannan, karena jika cuma 5 menit dokter akan kerepotan jika harus login lagi"*

(Responden 7, 2023)

Merujuk dari hasil wawancara diketahui ERM sudah menggunakan sistem logout otomatis, namun diketahui sistem logout otomatis masih teralalu lama dari yaitu 30 menit terakhir apabila tidak digunakan. Kerahasiaan data pasien tak hanya dilihat dari segi sistem keamanannya saja, namun juga berkaitan dengan kepada pihak mana saja data-data tersebut diberikan dan diperlukan untuk kepentingan tertentu. Menurut Harris (2013) dalam (Nawangsih, 2017) *confidentiality* adalah aspek untuk menjamin informasi tidak diungkapkan kepada individu, program, atau proses yang tidak berhak [9]. Dalam hal ini diperlukan pengawasan yang dapat mengatur kerahasiaan data pasien dalam E-RM, sehingga pengaksesan data pasien tidak dapat sembarang orang dapat melakukannya. Berdasarkan hasil wawancara dengan responden didapatkan kutipan sebagai berikut:

"*belum ada SOP khusus terkait keamanan ataupun penyelenggaraan E-RM"*

(Responden 2, 2023)

"*belum tahu"*

(Responden 3, 2023)

Hasil wawancara dari responden lain dari bidang RMIK menjelasakan bahwa SOP terkait keamanan E-RM masih dalam bentuk regulasi. Berikut adalah hasil kutipan wawancara dengan responden:

"keamanan secara sistem di IT sudah ada, di RM terkait dengan keamanan danhak akses, SOP masih dalam bentuk regulasi, SOP terkait hak akses itu yang diperlukan, butuh terus dikembangkan baik kuantitas maupun kualitas dan terus berproses dalam pengembangan"

(Responden 1, 2023)

Hasil wawancara tersebut sesuai dengan jawaban responden pada bidang IT yang Menjelaskan bahwa SOP terkait keamanan E-RM berada di bidang RMIK. Berikut adalah kutipan dari hasil wawancara responden pada bidang IT:

"SPO nya bukan di IT ya, tapi di rekam medis, IT hanya menyediakan aplikasi dan penyimpanan data, tapi untuk menjaga keamanan data di server iya, untuk masuk ruang server, untuk login server semua ada kebijakannya, tapi SPO nya seperti terkait pengguna tadi, itu berada di rekam medis"

(Responden 2, 2023)

Merujuk dari hasil wawancara diketahui rumah sakit belum memiliki SOP terkait penyelenggaraan rekam medis elektronik ataupun SOP khusus terkait keamanan dan kerahasiaan rekam medis elektronik sehingga rumah sakit perlu memiliki aturan atau kebijakan privasi rekam medis elektronik bagi pengguna. Kebijakan privasi dalam penerapannya mencakup tiga hal yaitu adanya ketegasan pembatasan pengguna data sebagai tujuan spesifik, mudah dipahami pemilik dan tidak adanya pengalihan tanggung jawab oleh pengguna. Kebijakan privasi tersebut lebih baik diimplementasikan dalam bentuk SOP oleh pihak internal rumah sakit [10]. Dengan penyusunan SOP organisasi dapat mendefinisikan tujuan dari kegiatan operasionalnya serta seluruh komponen terkait seperti alat atau data terkait operasional, aktivitas terkait kegiatan operasional maupun aktor yang terlibat dalam kegiatan operasional [9]. Dari hasil penelitian variabel kerahasiaan (*Confidentiality*) dapat disimpulkan bahwa aspek keamanan data pasien dalam implementasi rekam medis elektronik sudah terdapat login dengan menggunakan *username* dan *password* namun dalam penggunaan nya masih terdapat beberapa petugas yang belum melakukan penggantian username dan password secara berkala dan belum menggunakan karakter khusus atau kombinasi angka dan huruf. Hal tersebut dikarenakan kesibukan petugas dan berpotensi lupa dengan *username* dan *password*

"Ada"	(Responden 1, 2023)
"Ada, tergantung hak akses"	(Responden 3, 2023)
"Adanya fitur edit"	(Responden 6, 2023)

nya. Selain itu ditemukan permasalahan lain yaitu terkait belum adanya SOP penyelenggaraan rekam medis elektronik atau SOP khusus terkait keamanan dan kerahasiaan rekam medis elektronik.

3.2 Menganalisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik di Rumah Sakit X Berdasarkan Aspek Integritas (*Integrity*).

Integritas *(Integrity)* 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 personel atau proses yang tidak sah dan menjaga konsistensi data secara internal dan eksternal [9]. Integritas merupakan jaminan terhadap keakuratan data dan informasi yang ada dalam rekam medis elektronik, dan perubahan terhadap data hanya boleh dilakukan oleh orang yang diberi hak akses untuk mengubah [3]. Dalam penelitian ini integritas dapat dilihat dari adanya fitur edit dan hapus yang dapat digunakan untuk mengubah data pasien dalam sistem rekam medis elektronik. Dari hasil wawancara dengan responden dari aspek integritas diketahui di dalam sistem E-RM sudah terdapat fitur edit dan hapus sebagai bentuk pengeditan atau perubahan data. Berikut adalah hasil kutipan wawancara dengan responden.

Dari kutipan jawaban responden diatas, diketahui fitur edit dan hapus sudah ada dan tidak semua pengguna dapat menggunakan fitur tersebut, namun sesuai dengan hak akses masing-masing pengguna di dalam E-RM. Hal ini sesuai dengan jawaban responden pada bidang IT, berikut adalah kutipan jawaban responden dari bidang IT

> *"ada, jadi dalam pelaksanaannya seperti ini, resume medis apabila pasien pulang sudah tidak dapat di edit dan data pasien tidak dapat dihapus, tidak boleh kita hilangkan jejak atau riwayat dari seseorang pasien"*
>
> (Responden 7,2023)

> *"kalau misal mau edit sendiri itu masih 2 x 24 jam, tapi kita sementara begitu ada salah gak bisa langsung ngerubah harus lewat prosedur, tapi biasanya kalo salahnya diketahui dilapangannya edit langsung di lapangan tapi harus sepengetahuan atasannya"*
>
> (Responden 1, 2023)

Merujuk dari hasil wawancara diketahui sistem E-RM hanya terdapat fasilitas perubahan yaitu fitur edit. Hal ini sejalan dengan penelitian yang dilakukan oleh Ramadhanti (2022) yang menjelaskan bahwa di Rumah Sakit PHC Surabaya pada sistem E-RM tidak terdapat proses penghapusan karena kegiatan[11]

Penghapusan pada dasarnya tidak boleh dilakukan. Pencoretan dalam rekam medis elektronik tidak dapat dilakukan, sehingga diperlukan pengamanan yang lebih agar data tidak begitu saja dihapus atau diedit. [7]. Di Rumah Sakit X dalam perubahan datanya diketahui diberi batasan waktu yaitu 2 x 24 jam sesuai dengan prosedur yang berlaku. Berikut adalah kutipan wawancara dengan responden.

Pernyataan tersebut diperkuat dengan pernyataan pada bagian IT. Berikut adalah kutipan wawancara dengan bagian IT:

> "*ada, jadi gini sebenarnya kaya edit pasien kaya resume pasien, anamneses pasien begitu pasien pulang sudah gak bisa di edit kan itu ketentuannya, tapi dalam pelaksanaannya kan masih memungkinkan"*
>
> (Responden 7, 2023)

Merujuk dari hasil wawancara diketahui sistem E-RM dapat melakukan perubahan data pasien, apabila dokter ingin melakukan edit dari isi rekam medis elektornik pasien dapat dilakukan saat ditemukannya kesalahan, namun apabila perlu perubahan yang besar maka dokter harus melakukan perubahan isi data pasien dalam rekam medis elektronik sesuai dengan prosedur yang berlaku di Rumah Sakit. Hal ini sesuai dengan penelitian yang dilakukan oleh [12] menjelaskan bahwa RSUP Nasional Dr. Cipto Mangkusumo Jakarta apabila dokter ingin melakukan perubahan isi dari rekam medis elektronik memerlukan persetujuan dari bagian rekam medis yaitu kepala sub bagian rekam medis, penanggung jawab pelayanan rekam medis, dan kepal instansi rekam medis dan admisi.

Dari hasil penelitian variabel integritas *(integrity*) dapat disimpulkan bahwa aspek keamanan data pasien dalam implementasi rekam medis elektronik di Rumah Sakit X dapat diakatakan cukup baik. Karena di dalam sistem E-RM sudah terdapat fitur edit yang hanya dapat digunakan oleh petugas sesuai dengan hak aksesnya berdasarkan tugas, wewenang dan tanggung jawabnya dalam pelayanan di rumah sakit, selain itu dengan tidak dapat dihapusnya data pasien yang karena hal tersebut tidak diperbolehkan. Perubahan data pasien dalam rekam medis elektronik di Ruamh Sakit X tidak serta merta dapat dilakukan, namun harus sesuai dengan prosedur yang berlaku demi menjaga integritas data pasien dalam rekam medis elektronik.

3.3 Menganalisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik di Rumah Sakit X Berdasarkan Aspek Autentikasi (*Autentication*).

Autentikasi atau *authentication* merupakan aspek keamanan data pasien yang berkaitan dengan akses informasi atau bagaimana sistem menyatakan keabsahan untuk pengguna dapat mengakses data didalam sistem [5]. Metode yang dapat digunakan untuk autentikasi pengguna dapat menggunakan kata sandi, nomor identitas (PIN), biometrik dan lain sebagiannya [9]. Berdasarkan hasil wawancara dan observasi sudah menerapkan penggunaan *username* dan *password* untuk keamanan data pasien, petugas yang akan menggunakan ERM, wajib menginputkan *username* dan *password* sebagai bentuk verifikasi sistem bahwa petugas tersebut memiliki hak akses terhadap ERM.

Tidak hanya dengan penggunaan *username* dan *password*, cara lain yang dapat digunakan untuk menjaga keamanan data pasien dari aspek autentikasi adalah dengan penerapan tanda tanggan elektronik. Penyelenggaraan rekam medis eletronik di faslitas pelayanan kesehatan dapat dilengkapi dengan tanda tangan elektronik. Tanda tangan elektronik digunakan sebagai alat verifikasi dan autentikasi atas rekam medis elektronik dan identitas penanda tangan [3]. Dari hasil penelitian di Rumah Sakit X terkait dengan tanda tangan elektronik diketahui sudah diterapkan secara optimal. Hal tersebut dibuktikan dari hasil wawancara dengan responden sebagai berikut:

> "*sudah ada, tanda tangan elektronik dilakukan dengan cara scan tanda tangandi realisasikan dengan username dan password dokter, disini dokter cukup menginputkan kode dokter untuk tanda tangan"*
>
> (Responden 1, 2023)

> *"sudah ada, tapi untuk pasien masih belum ada, untuk pasien yang membutuhkan tanda tangan masih menggunakan tanda tangan manual"*
>
> (Responden 2, 2023

Pernyataan tersebut diperkuat dengan pernyataan pada bagian IT. Berikut Adalah kutipan wawancara dengan bagian IT.

> "*sudah ada, tapi rekam medis elektronik terkait dengan tanda tangan elektornik belum ada regulasinya, apakah tanda tangan nya di scan, apakah dibuat barcode belum ada regulasinya, untuk Lembaga yang berhak mengeluarkan sertifikasi terkait tanda tangan elektronik itu sudah ada"*
>
> (Responden 7, 2023)

Tanda tangan elektronik adalah tanda tangan yang terdiri atas informasi elektronik yang diletakkan, terasosiasi atau terkait dengan infromasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi. Penanda tangan adalah subjek hukum yang terasosiasikan atau terkait dengan tanda tangan elektronik [13]. Menurut pasal 11 UU ITE, tanda tangan elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan

Dari beberapa persyaratan terkait tanda tangan elektronik dapat disimpulkan tanda tangan elektronik yang memiliki kekuatan hukum merupakan tanda tangan yang dibuat dengan menggunakan jasa penyelenggara sertifikasi elektronik, dan hal tersebut sudah di terapkan di Rumah Sakit X. Hal ini sejalan dengan penelitian yang dilakukan oleh [5]tanda tangan digital di fasilitas pelayanan kesehatan seperti rumah sakit memiliki sistem enkripsi yang aman, dapat menghindari risiko pemalsuan tanda tangan atau penyalahgunaan pihak yang tidak bertanggung jawab, efisien dan dilindungi oleh penjamin.

Dari hasil penelitian variabel autentikasi *(Autentication)* dapat disimpulkan bahwa aspek keamanan data pasien dalam implementasi rekam medis elektronik sudah menerapkan tanda tangan elektronik bagi dokter pemberi asuhan yang telah tersertifikasi sebagai salah satu bentuk kekuatan hukum dalam penyelenggaraan rekam medis elektronik. Dari hasil penelitian diketahui formulir yang membutuhkan tanda tangan pasien masih dilakukan secara manual.

3.4 Menganalisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik di Rumah Sakit X Berdasarkan Aspek Ketersediaan *(Availability)*.

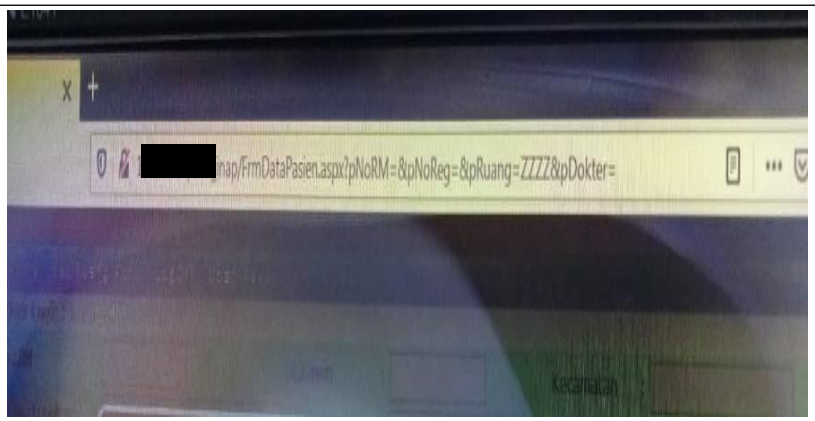
Ketersediaan atau *availability* merupakan aspek yang menjamin data akan tersedia saat dibutuhkan kapanpun dan dimanapun bagi user yang memiliki hak akses [9]. Penyimpanan rekam medis elektronik harus menjamin keamanan, keutuhan, kerahasiaan, dan ketersediaan data rekam medis elektronik [3]. Rekam medis elektronik sebagai alat komunikasi diwajibkan untuk selalu tersedia secara cepat serta dapat menampilkan kembali data yang terlah tersimpan sebelumnya. Dari hasil penelitian di Rumah Sakit X terkait dengan aspek ketersediaan ERM diketahui rekam medis elektronik hanya dapat diakses di lingkungan dan jaringan rumah sakit.

Hal tersebut dibuktikan dengan hasil wawancara dengan responden sebagai berikut:

> *"gak bisa, hanya bisa di lingkungan rumah sakit dengan internet rumah sakit"*
>
> (Responden 3, 2023)

Hasil wawancara dengan responden tersebut diperkuat dengan hasil wawancara dengan responden pada bagian IT, yaitu sebagai berikut:

> *"tidak bisa, hanya dapat diakses di rumah saki dengan menggunakan VPN dan VPN sendiri sudah diatur oleh IT ya, jadi tidak serta merta setiap orang bisa mengaksesnya "*
>
> (Responden 7, 2023)



Gambar 2. Jaringan Internet Yang Dapat Digunakan Untuk Mengakses ERM

Berikut adalah gambar jaringan yang dapat diakses pengguna untuk membua sistem ERM, dimana sistem rekam medis elektronik di Rumah Sakit X hanya bisa diakses dengan jaringan tersebut dan tidak bisa diakses dengan menggunakan jaringan internet lain selaian miliki rumah sakit yang telah di setting oleh pihak IT.

Merujuk dari hasil wawancara dan observasi tersebut sesuai dengan penelitian yang dilakukan oleh [11] menjelaskan bahwa pengaksesan rekam medis hanya dapat dilakukan menggunakan jaringan internet di Rumah Sakit PHC Surabaya. Ketersediaan merupakan jaminan data dan infromasi yang ada dalam rekam medis elektronik dapat diakses dan digunakan oleh orang yang telah memiliki hak akses yang ditetapkan oleh pimpinan fasilitas pelayanan kesehatan [3].

> "*semua petugas yang memiliki hak akses bisa mengakses informasi pelayanan pasien sesuai dengan hak aksesnya"* (Responden 1, 2023)
>
> *"sepertinya iya bisa dilihat"* (Responden 3, 2023)
>
> *"iya, semua poli bisa mengakses data pelayanan pasien dengan mudah"*
>
> (Responden 5, 2023)

Hasil jawaban dari responden di atas diperkuat dengan, hasil wawancara dengan responden bidang IT, berikut adalah hasil kutipan wawancara dengan responden.

> "*gak bisa, hanya bisa di lingkungan rumah sakit dengan internet rumah sakit"*
>
> (Responden 3, 2023)
>
> "*iya mudah diakses, tapi juga mengacu pada level language dari username dan password tadi ya, kelebihan dari elektronik adalah mudah diakses. Untuk batas waktu kembali ke kebijakan rekam medis, karena rekam medis yang memiliki kewenangan bagaimana data pasien diakses, bagaimanan penyimpannanya. Tapi untuk saat ini masih belum ada batas waktunya"*
>
> (Responden 7, 2023)

Merujuk dari hasil wawancara diketahui semua petugas yang memiliki hak akses atas ERM dapat mengakses ERM dengan mudah. Untuk saat ini ERM dapat diakses tanpa adanya batasan waktu bagi user. Dalam undang-undang RI nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dijelaskan bahwa setiap penyelenggaraan sistem elektronik wajib mengoperasikan sistem elektronik yang memenuhi

persyaratan minimum salah satunya adalah dapat menampilkan kembali informasi elektronik dan/ atau serta dapat melindungi ketersediaan, keutuhan, keautentikan, kerahasiaan dan keteraksesan infromasi elektronik dalam penyelenggaraan sistem elektronik tersebut [14].

Dari hasil penelitian variabel ketersediaan *(Availability)* dapat disimpulkan bahwa aspek keamanan data pasien dalam implementasi rekam medis elektronik dilihat dari pengaksesan ERM sudah baik, karena ERM hanya dapat diakses dilingkungan rumah sakit dengan menggunakan jaringan internet atau VPN yang telah di setting oleh pihak IT, demi menjaga keamanan data pasien. Selain itu kemudahan bagi professional pemberi asuhan dalam mengakses informasi pelayanan pasien sudah berjalan dengan baik, namun terdapat kelemahan dimana semua poli dapat mengakses data pelayanan pasien.

3.5 Menganalisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik di Rumah Sakit X Berdasarkan Aspek Akses Kontrol *(Acess Control)*.

Akses kontrol atau acess control merupakan aspek yang berkaitan dengan bagaimana penganturan akses pengguna terhadap sistem informasi, proses ini dilakukan untuk memastikan hanya petugas yang memiliki hak akses yang dapat menggunakan sistem informasi kesehatan [5]. Dengan adanya akses kontrol dapat menjaga keamanan data pasien dengan cara menggunakan *username dan password* untuk mengantur pengguna ERM serta membatasi hak akses user. Hasil penelitian didapatkan hasil hak akses dari setiap pengguna berbeda sesuai dengan tugas, wewenang dan tanggung jawab. Berikut adalah hasil wawancara dengan responden terkait dengan hak akses ERM.

> "*hak akses yang mengantur dari tim IT, usulan dari bagian terkait"*
>
> (Responden 2, 2023)

Pernyataan dari responden tersebut diperkuat dengan jawaban responden dari bidang IT, berikut adalah hasil wawancara dari dari bidang IT.

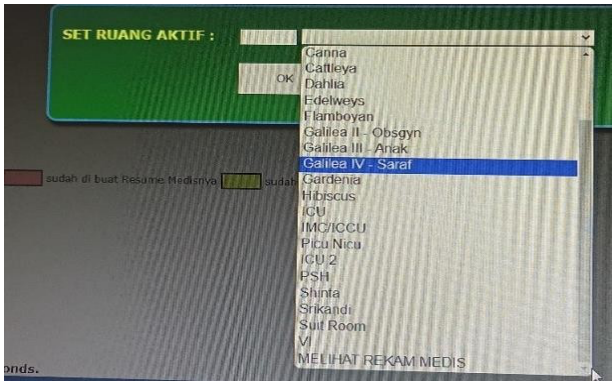
> "*pembatasan hak akses di setting dari username dan password"*
>
> (Responden 3, 2023)

Merujuk dari hasil wawancara diketahui Rumah Sakit X dalam penganturan hak akses yang digunakan adalah dengan penerapan *username dan password* yang telah di atur oleh pihak IT berdasarkan usulan masing-masing bidang. Hal ini sesuai dengan penelitian yang dilakukan oleh [11] menjelaskan bahwa penganturan hak akses pengguna HIS sesuai dengan tugas dan wewenangnya masing-masing. Berdasarkan wawancara dengan responden diketahui ERM memiliki tampilan yang sama walaupun dengan hak akses yang berberda. Berikut adalah hasil kutipan wawancara dengan responden.

> "*tampilan sama"*
>
> (Responden 3, 2023)

Pernyataan dari responden bidang IT, diketahui tampilan menu semua ERM sama namun pada menu-menu yang dibatasi hak aksesnya tidak dapat digunakan. Berikut adalah hasil wawancara dengan responden bidang IT:

> "*untuk tampilan menu semua, hanya ada fitur yang sudah diatur agar tidak bisa digunakan, misalkan pada petugas rekam medis hanya bisa melihat tidak bisa menggunakan fitur edit dan dokter bisa melihat dan mengedit"*
>
> (Responden 7, 2023)



Gambar 3. Set Ruang Aktif Pada Menu Rekam Medis Elektronik

Berikut adalah gambar set ruang aktif yang dapat diakses pengguna ERM untuk melihat data pasien, dimana pada petugas bisa melihat infromasi terkiat pelayanan pasien pada masing-masing ruang perawatan atau hanya melihat rekam medis pasien. Namun tidak semua fitur bisa digunakan oleh petugas, seperti petugas rekam medis yang hanya bisa melihat rekam medis pasien di masing - masing ruang pelayanan namun tidak bisa mengedit atau mengisi rekam medis elektronik dan dokter bisa meliat, mengedit, dan mengisi rekam medis elektronik pasien.

Merujuk dari hasil wawancara dan observasi diketahui tampilan menu pada sistem ERM memiliki tampilan yang sama, pembatasan hak akses pada tampilan diatur dengan cara menyeting fitur pada ERM agar tidak dapat digunakan oleh pengguna yang tidak berkepentingan. Dari hasil penelitian diketahui belum adanya pengaturan tampilan menu yang berbeda sesuai dengan hak akses dari masing – masing pengguna. Hal ini tidak sejalan dengan penelitian yang dilakukan oleh Sofia dkk (2022) yang menjelaskan bahwa rekam medis elektronik harus memiliki tampilan menu yang berbeda [5].

Dari hasil penelitian variabel akses control *(access control)* dapat disimpulkan bahwa aspek keamanan data pasien dalam implementasi rekam medis elektronik diketahui untuk membatasi hak akses sistem ERM menggunakan *username dan password* sesuai dengan tugas, wewenang dan tanggung jawab masing-masing pengguna ERM. Hasil penelitian pada aspek ini ditemukan semua tampilan menu pada ERM memiliki tampilan yang sama, kontrol akses dilakukan dengan menyeting fitur agar tidak dapat digunakan oleh pihak yang tidak berkepentingan.

3.6 Menganalisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik di Rumah Sakit X Berdasarkan Aspek Akses Nir-Sangkal *(Nonrepudiation)*

Nir-sangkal atau *nonrepudiation* merupakan bagaimana sistem dapat merekam jejak perubahan data yang dilakukan oleh pengguna [2]. 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, verivikasi, pengujian, dan pemeriksaan lainya [15]. Dari hasil penelitian yang telah dilakukan berdasarkan hasil wawancara sudah terdapat history bagi pengguna yang menggunakan ERM. Berikut adalah hasil kutipan wawancara dengan responden

> *"sudah ada, apa saja yang dibuka atau diakses akan tersimpan di log data"*
>
> (Responden 1, 2023)

Pernyataan tersebut diperkuat dengan jawaban dari responden IT, berikut adalah hasil kutipan wawancara dengan responden pada bidang IT

> "*ada riwayat log nya, misal yang mengedit siapa, sekarang kan rekam medis sudah ada audit trail, itu salah satu bagaimana kita melakukan trasik terhadap data-data yang dihapus, siapa yang menghapus dan kenapa dihapus"*
>
> (Responden 7, 2023)

Merujuk dari hasil wawancara diketahui di Rumah sakit X dalam sistem ERM sudah terdapat riwayat pengguna ERM terkait apa saja yang di akses dan di edit. Hal ini sejalan dengan penelitian yang dilakukan oleh [16] 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 rekam medis elektronik. Sistem audit keamanan data merupakan cara untuk dapat mengetahui siapa saja yang mengakses infromasi dan perubahan apa saja yang telah dilakukan pada data pasien. Berdasarkan wawancara diketahui belum melakukan audit sistem. Hal tersebut diperkuat dengan hasil wawancara dengan responden sebagai berikut.

> "*belum"* (Responden 4, 2023)

Namun dari hasil jawaban responden lain menjelaskan sudah pernah dilakukan audit dengan penilaian maturnity index. Berikut adalah hasil kutipan wawancara dengan responden

> "*Audit ERM secara internal belum, tapi sudah penilaian maturnity index danpenelitian"*
>
> (Responden 1, 2023)
>
> "*Sudah pake HIMSS"* (Responden 7, 2023)
>
> "*sudah ada, apa saja yang dibuka atau diakses akan tersimpan di log data"*
>
> (Responden 1, 2023)

Merujuk dari hasil wawancara diketahui sudah dilakukan audit ERM dengan menggunakan HIMSS dan penilaian dengan *maturnity index*. Namun belum pernah melakukan audit sistem ERM secara internal. Menurut penelitian yang dilakukan oleh [5] penyelenggara sistem elektronik wajib menyediakan rekam jejak audit terhadap seluruh kegiatan penyelenggaraan sistem elektronik. Rekam jejak audit sebagaimana dimaksud digunakan untuk keperluan pengawasan, penegakkan hukum, penyelesaian sengketa, verifikasi, pengujian dan pemeriksaan lainnya.

Dari hasil penelitian variabel nir-sangkal *(nonrepudiation)* dapat disimpulkan bahwa aspek keamanan data pasien dalam implementasi rekam medis elektronik dari aspek nir-sangkal didapatkan hasil sudah baik karena sudah terdapat riwayat bagi pengguna yang mengakses ERM di dalam log data sehingga dapat diketahui siapa saja yang mengakses atau melakukan pengeditan pada data pasien. Audit sistem ERM sudah dilakukan dengan menggunakan penilaian maturnity index dan HIMSS, namun belum dilakukan audit ERM secara internal.

4. KESIMPULAN

1. Aspek kerahasiaan *(Confidentiality)* dapat disimpulkan bahwa aspek keamanan data pasien dalam implementasi rekam medis elektronik sudah terdapat login dengan menggunakan *username dan password* namun masih terdapat beberapa petugas yang belum melakukan penggantian *username dan password* secara berkala dan belum menggunakan karakter khusus atau kombinasi angka dan huruf. belum adanya SOP penyelenggaraan rekam medis elektronik atau SOP khusus terkait keamanan dan kerahasiaan rekam medis elektronik.
2. Aspek integritas *(integrity)* dapat disimpulkan bahwa aspek keamanan data pasien dalam implementasi rekam medis elektronik dalam sistem E-RM sudah terdapat fitur edit yang hanya dapat digunakan oleh petugas sesuai dengan hak aksesnya berdasarkan tugas, wewenang dan tanggung jawabnya dalam pelayanan di rumah sakit. Rumah Sakit tidak serta merta dapat dilakukan, namun harus sesuai dengan prosedur yang berlaku demi menjaga integritas data pasien dalam rekam medis elektornik.

3. Aspek autentikasi *(Autentication)* dapat disimpulkan bahwa aspek keamanan data pasien dalam implementasi rekam medis elektronik sudah menerapkan tanda tangan elektronik bagi dokter pemberi asuhan yang telah tersertifikasi sebagai salah satu bentuk kekuatan hukum dalam penyelenggaraan rekam medis elektronik. Formulir yang membutuhkan tanda tangan pasien masih dilakukan secara manual.
4. Aspek ketersediaan *(Availability)* dapat disimpulkan bahwa aspek keamanan data pasien dalam implementasi rekam medis elektronik dilihat dari pengaksesan ERM sudah baik, karena ERM hanya dapat diakses dilingkungan rumah sakit dengan menggunakan jaringan internet atau VPN yang telah di setting oleh pihak IT, demi menjaga keamanan data pasien. Kemudahan bagi professional pemberi asuhan dalam mengakses informasi pelayanan pasien sudah berjalan dengan baik, namun terdapat kelemahan dimana semua poli dapat mengakses data pelayanan pasien.
5. Aspek akses control *(access control)* dapat disimpulkan bahwa aspek keamanan data pasien dalam implementasi rekam medis elektronik diketahui untuk membatasi hak akses sistem ERM menggunakan *username dan password* sesuai dengan tugas, wewenang dan tanggung jawab masing- masing pengguna ERM. Hasil penelitian pada aspek ini ditemukan semua tampilan menu pada ERM memiliki tampilan yang sama, kontrol akses dilakukan dengan menyeting fitur agar tidak dapat diguankan oleh pihak yang tidak berkepentingan.

REFERENSI

[1] KOMINFO, "Peraturan Menteri Komunikasi dan Informatika Republik Indonesia," Jakarta, 2012.

[2] D. R. A. Tiorentap and H. Hosizah, "'Aspek keamanan informasi dalam penerapan rekam medis elektronik di Klinik Medical Check-Up MP.' 4th Proceeding Perspektif Implementasi FHIR," 2020, pp. 53–66. [Online]. Available: https://prosiding.esaunggul.ac.id/index.php/FHIR/article/view/71/6

[3] KEMENKES RI, "Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 Tentang Rekam Medis," *Braz Dent J*, vol. 33, no. 1, pp. 1–12, 2020.

[4] R. Musyarofah, S. R. A., Bisma, "Pembuatan Standard Operating Procedure (SOP) Keamanan Informasi Berdasarkan Framework ISO/IEC 27001: 2013 dan ISO/IEC 27002: 2013 pada Dinas Komunikasi dan Informatika Pemerintah Kota Madiun.," *J. Emerg. Inf. Syst. Bus. Intell.*, vol. 1, no. 1, pp. 43–50, 2020.

[5] S. [Sofia, E. T. Ardianto, N. Muna, and S. Sabran, "Analisis Aspek Keamanan Informasi Data Pasien Pada Penerapan RME di Fasilitas Kesehatan. Jurnal Rekam Medik & Manajemen Informasi Kesehatan," pp. 94–103, 2022, [Online]. Available: https://doi.org/10.47134/rmik.v1i2.29

[6] Cloudmatika, "Pahami 5 Prinsip Keamanan Jaringan yang Harus Dipatuhi," 2022. [Online]. Available: https://cloudmatika.co.id/blog-detail/prinsip-keamanan-jaringan

[7] N. Nugraheni, S. W., Nurhayati, "Aspek Hukum Rekam Medis Elektronik di RSUD Dr Moewardi. In Prosiding Seminar Nasional Unimus," 2018.

[8] E. M. [Safitri and A. S. Larasati, "Analisis Keamanan Sistem Informasi E- Banking Di Era Industri 4.0: Studi Literatur.," *J. Ilm. Teknol. Inf. Dan Robot.*, vol. 2, no. 1, pp. 12–16, doi: https://doi.org/10.33005/jifti.v2i1.25.

[9] N. Nawangsih, "Pembuatan Standard Operasional Prosedur Kontrol Akses Physical & Logical Pada Aplikasi System Informasi Rumah Sakit (SIM RS) Menggunakan Kerangka Oktave, FMEA dan Kontrol ISO 27002:2013."

[10] Y. Fitriyah, "Analisis Tingkat Kesiapan implmentasi Tanda Tangan Digital Untuk Autentikasi Dokumen Rekam Medis ELektronik di Instalasi Rawat Jalan RSUD Kota Yogyakarta," *J. Inf. Syst. Public Heal.*, vol. 7, no. 2, p. 53, 2022, doi: https://doi.org/10.22146/jisph.73666.

[11] A. T. [Ramadhanti, "Analisis Aspek Keamanan Informasi Pasien Dalam Penerapan Rekam Medis Elektronik Di Rumah SAkit PHC Surabaya," vol. 8, no. 5, 2022.

[12] E. N. Hidayah, "Analisis Aspek Keamanan Data Pada Hospital Information System (HIS) Dalam Penerapan Rekam Medis Eleketornik di RSUP Nasional DR.Cipto Mangkusumo Jakarta," *J. Kesehat. Lingkung. Indones.*, no. 22, p. 2, 2023.

[13] UU RI, "UU No. 19 Tahun 2016," Jakarta, 2016.

[14] UUD ITE, "Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik," Jakarta, 2008.

[15] PP RI, "Peraturan pemerintah Repbulik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik," Jakarta.

[16] 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*, vol. 3, no. 1, pp. 20–28, 2021.