BAB IV
PEMBAHASAN

A. Hasil Karya Ilmiah

Keamanan komputer terutama pada bidang kesehatan meliputi 6 faktor ialah *privacy* ataupun *confidentiality, integrity, authentication, availability, access control* serta *non repudiation.* Hal utama berdasarkan faktor *privacy* ataupun *confidentiality* ialah penjagaan informasi berdasarkan pihak yang tidak mempunyai hak dalam melakukan akses informasi. *Integrity* berhubungan sama perubahan informasi. *Authentication* berkaitan sama akses pada informasi. *Availability* ataupun ketersediaan ialah faktor yang memberikan penekanan kepada ketersediaan informasi jika diperlukan sama pihak terkait. *Access control* ialah faktor yang memberikan penekanan sama metode pengaturan akses pada informasi. *Non repudiation* erat hubungannya sama suatu transaksi ataupun pergantian informasi.

1. Aspek Kerahasiaan

UU 17 tahun 2023 mengenai aspek rahasia mungkin merujuk pada Undang-Undang Nomor 17 Tahun 2023 tentang Perlindungan Data Pribadi. Undang-undang ini umumnya mengatur tentang bagaimana data pribadi individu harus dilindungi, termasuk aspek kerahasiaan dan keamanan dalam pengelolaan data tersebut. Beberapa poin yang umumnya diatur dalam undang-undang ini meliputi: Definisi data pribadi dan jenis data yang dilindungi. Kewajiban perusahaan atau entitas yang mengelola data pribadi untuk menjaga kerahasiaan dan keamanan data, Hak individu atas data pribadi mereka, seperti hak untuk mengakses, memperbaiki, atau menghapus data pribadi mereka, Persyaratan untuk memperoleh persetujuan dari individu sebelum mengumpulkan atau memproses data pribadi mereka, Prosedur yang harus diikuti dalam kasus pelanggaran keamanan data, Undang-undang semacam ini biasanya diberlakukan untuk

melindungi privasi individu dalam era digital di mana pengumpulan dan pengolahan data pribadi sangat meluas (Presiden RI, 2023).

Berdasarkan wawancara terhadap Kepala SDM, mengatakan bahwa Hak akses SIMRS diberikan satu mitra kerja hingga memang setiapnya mempunyai kode rahasianya. *Username* serta *Password* dipakai dalam memberikan bukti kalau pengguna mempunyai wewenang dalam menggunakan serta masuk pada sistem. Maka dari itu semua pengguna sebelum, masuk pada sistem informasi wajib mengetik atau memasukan *username* serta *password*. Dalam menjauhi agar sistem tidak diakses sama pengguna yang tidak mempunyai wewenang, maka wajib dikontrol sama mengkombinasikan kontrol preventif serta pendeteksian.

Tabel 4. 1 Wawancara Aspek Kerahasiaan

Sub kategori	Pertanyaan	Hasil Wawancara Informan
Aspek Kerahasiaan	"Siapa yang bertanggung jawab atas pengaturan dan pemeliharaan kontrol akses keamanan untuk menjaga kerahasiaan data	*"bahwa Hak akses SIMRS diberikan satu mitra kerja sehingga memang masing-masing memiliki kode rahasianya"* Kepala SDM
	"Bagaimana SIMRS mengatasi risiko akses tidak sah atau penyalahgunaan data pasien dalam SIMRS?"	*"Untuk tidak terjadinya penyalagunaan data pasien dalam sistem SIMRS diberikan hak akses masing-masing pengguna, jadi pengguna yang tidak memiliki hak askes tidak dapat masuk ke SIMRS"* Staff IT

Fakta bahwa sistem informasi memerlukan *username* dan *password* untuk login menunjukkan bahwa privasi terjamin. Keamanan informasi merupakan permasalahan sumber daya manusia sekaligus isu sekunder terkait teknologi. Manusia sebagai pengguna itu sendiri. Salah satu risiko keamanan terbesar bagi banyak industri, termasuk industri kesehatan, adalah teknologi yang dijalankan. Mayoritas pelanggaran

keamanan disebabkan oleh kesalahan atau kecerobohan manusia, dan dapat berakibat fatal bagi profesional kesehatan. Tanpa kesadaran pengguna akan keamanan data, kata sandi dan nama pengguna aplikasi tidak cukup untuk melindungi kerahasiaan data pasien. Oleh karena itu, pengguna sistem informasi harus sadar akan keamanan untuk menjaga datanya.

Pentingnya memahami keamanan informasi untuk melindungi privasi data, mengurangi kejahatan dunia maya dan kejahatan online lainnya, dan mengatasi masalah keamanan informasi lainnya. Hal ini dapat mengakibatkan banyak kasus. Rekam medis yang digunakan untuk tujuan yang tidak berkaitan dengan pemberian pelayanan kesehatan dan juga catatan kesehatan. Karena pelayanan kesehatan yang harus merawat pasien yang sama dapat mengakses perangkat elektronik secara luas, terdapat potensi kebocoran yang cukup besar.

Dalam hal ini juga perlu adanya pihak-pihak yang bertanggung jawab atas pengelolaan serta keamanan data pada SIMRS, sehingga dengan hasil wawancara kepada Staff IT, yang paling utama itu adalah unit IT kemudian dari unit rekam medik selanjutnya seluruh pengguna dari SIMRS. Mitra kerja yang diberikan hak akses tentunya mempunyai tanggung jawab terhadap data pasien itu sendiri. Data rekam medis yang berisikan riwayat kesehatan pasien yang ialah dokumen rahasia wajib selalu dilindungi kerahasiaanya.

2. Aspek Integrasi

Integritas adalah komponen perubahan informasi; segala jenis modifikasi dapat dilakukan oleh sistem atau catatan kesehatan elektronik, dan sistem yang ada dapat mengawasinya. Paraf dokter atau tenaga kesehatan harus dicantumkan. Sehingga, diperlukan keamanan atau perlindungan yang lebih besar, terutama untuk menghapus data dari rekam medis elektronik dan mengumumkan revisi apa pun.

Berdasarkan hasil wawancara dari aspek integritasi, Hal itu bisa dinyatakan kalau faktor integritas sudah cukup baik. Sehingga dengan adanya perubahan data atau kesalahan data dapat dilakukan dengan tanpa adanya kekhawatiran dari pihak yang berwewenang. Hal ini juga berhubungan sama mutu data yang bersangkutan serta bisa dipengaruhi pada mutu layanan kesehatan yang diberikan.

Tabel 4. 2 Wawancara Aspek Integrasi

Sub kategori	Pertanyaan	Hasil Wawancara Informan
Aspek Integrasi	"apakah SIMRS memiliki kemampuan untuk mengintegrasikan system keamanan pihak ketiga seperti deteksi farewall, untuk mempertimbangkan keamanan data?"	*"Untuk keamanan data SIMRS sih kita untuk akses publik kita batasi dengan firewall kita menggunakan cloud fire untuk pembatasannya nek secara akses publik loh, tapi secara internal untuk keamanan sih kita sudah memisahkan antara jaringan yang digunakan untuk wifi publik sama jaringan internal rumah sakit jadi untuk keamanan seperti itu kalo yang disisi SIMRS untuk yang internal ya untuk yang eksternal kita sudah memakai cloud fire sebagai deteksi firewall nya"* Staff IT
	"bagaimana jika petugas lupa atau secara sengata tidak mengisikan beberapa kolom data pada SIMRS sehingg petugas langsug menimpan data yang diinputkan, apakah hal ini dapat diedit kembali ?"	*"bisa diedit, ketika daftar pasien baru jika tidak di isi lengkap kolom yang tersedia tidak bisa disimpan dan misalkan ada kesalahan dan mau dibenarkan masih bisa di edit di menu edit atau tidak ada pilihan editnya itu biasanya petugas konfirmasi ke IT"* Petugas Rekam Medik

3. Aspek Autentikasi

Berdasarkan hasil wawancara aspek autentikasi, Salah satu fitur keamanan yang berkaitan dengan akses informasi adalah Autentikasi. Di sini, pengguna perlu memberikan bukti kalau dia ialah pengguna yang sah.

Sistem keamanan biometrik beroperasi berdasarkan sejumlah prinsip panduan, salah satunya adalah keakuratan penerapan biometrik, dimana teknologi biometrik akan meningkatkan akurasi identifikasi individu secara

signifikan. Selanjutnya, prinsip operasional termasuk sistem pengenalan wajah (*face id*) ialah diantara teknologi biometrik yang banyak dipakai kala ini.

Tabel 4. 3 Wawancara Aspek Autentikasi

Sub kategori	Pertanyaan	Hasil Wawancara Informan
Aspek Autentikasi	"Apa jenis autentikasi yang digunakan pada SIMRS untuk memastikan bahwa pengguna yang mengakses sistem adalah pengguna yang telah diberikan hak akses?"	*"untuk autentikasi kita menggunakan username dan pin ya nanti pin nya kita menggunakan metode hash atau md5 untuk enkripsinya"* jawabnya. Staff IT
	"Bagaimana manajemen kata sandi dilakukan dalam SIMRS, termasuk kebijakan yang mengatur kompleksitas kata sandi serta password maupun terhadap siklus penggantian?"	*"manajemen kata sandi, nah itu di SIMRS kita sih, setiap petugas bisa mengedit sendiri sendiri. User ee Passwordnya mereka bisa mengedit sesuka mereka, tidak ada dari aturannya, karna di SIMRS nya sudah menu nya untuk usernya ngedit sendiri"* Kepala IT
		"Selama kerja 8 tahun hingga sekarang belum ada pergantian password dan terdapat adanya untuk kebijakan SOP ada di SDM" Petugas IT
	"Faktor apa yang dipertimbangkan saat menetapkan hak akses integrasi data?	*"yang dipertimbangkan adalah unitnya, unit sama posisinya jadi dia sebagai struktural atau sebagai pelaksana. Kalo sebagai struktural berarti banyak hak akses yang kita berikan poin-poin nya termasuk dari keungan dan lainnya itu kita buka kan tapi kalo dia eee...sebagai staff itu hanya sebatas unitnya saja. Jadi yang bisa melihat yaa hanya unitnya ya misalnya unit farmasi berarti hanya bisa melihat di farmasi nya itu tetapi tidak bisa melihat ke laporan unit lainnya seperti itu, jadi kami melihatnya dari struktural jabatan sama unitnya"*

		Kepala SDM

Diketahui tidak adanya kebijakan serta aturan minimal yang jelas dalam pembuatan password pada setiap pengguna SIMRS. Dan menurut salah satu informan yang telah diwawancarai mengaku tidak pernah mengganti password selama ia bekerja, yang dimana hal kecil seperti ini perlu menjadi perhatian pihak rumah sakit khususnya pada pengguna itu sendiri.

Tanpa aturan yang jelas, kemungkinan besar banyak petugas yang akan menggunakan password yang mudah ditebak seperti tanggal lahir, nama hewan peliharaan, atau bahkan kata-kata umum. Password yang lemah ini akan menjadi sasaran empuk bagi hacker untuk melakukan peretasan. Yang dimana menjadi rentan terhadap serangan *cyber*.

Jika SIMRS berhasil diretas, maka data pasien yang sangat sensitif seperti riwayat penyakit, hasil lab, dan informasi pribadi lainnya dapat dengan mudah dicuri, diubah, atau disebarluaskan tanpa izin. Hal ini dapat mengakibatkan penyalahgunaan data, penipuan identitas, dan kerugian finansial bagi pasien.

4. Aspek Ketersediaan

Berdasarkan hasil wawancara pada aspek ketersediaan, Pada aspek ketersediaan adalah pada seberapa cepat (*just in time*) informasi tersedia bila dihubungkan oleh pihak-pihak terkait

Tabel 4. 4 Wawancara Aspek Ketersediaan

Sub kategori	Pertanyaan	Hasil Wawancara Informan
Aspek Ketersediaan	"Bagaimana data yang telah terinputkan dapat ditampilkan kembali dengan cepat ketika dibutuhkan?"	*"tinggal data yang dibutuhkan apa, misal yang dibutuhkan identitas pasien baru, hasil rontgen lab, ekg, diagnosa dll tinggal mengetikan nomor rm"* Petugas Rekam Medik
	"Bagaimana SIMRS memastikan ketersediaan data pasien dalam situasi	*"kalo di kita, Kita menggunakan data manual dulu ya jadi secara berkala itu ada untuk menekstrak*

	darurat atau kegagalan sistem yang tidak terduga?”	*data pasien ke excel jadi pas klo SIMRS down gabisa bener-bener gabisa diakses itu kita menggunakan data manual itu pake excel”* Staff IT

Dalam hal tersebut, akses ketersediaan yang dimiliki RSU Rajawali Citra sudah terlaksana dengan baik. Aspek ketersediaan juga bisa dibuktikan sama hubungan sama organisasi lainnya khusunya BPJS, ialah memudahkan tahapan klaim pasien BPJS.

Faktor *availability* dalam pelaksanaan rekam medis elektronik di sarana kesehatan berpedoman sama ketersediaan sistem informasi kesehatan tersebut secara keseluruhan. Beberapa poin yang perlu dianalisis dalam konteks ini termasuk:

Infrastruktur Teknologi: Ketersediaan perangkat keras serta perangkat lunak yang dibutuhkan dalam mendorong sistem rekam medis elektronik (RME). Ini mencakup server, jaringan komunikasi, dan perangkat pengguna akhir seperti komputer atau tablet.

Ketersediaan Akses: Sistem RME harus dapat diakses oleh semua personil yang berwenang di fasilitas kesehatan, termasuk dokter, perawat, dan staf administrasi. Ini mencakup keamanan akses yang memadai serta pengaturan hak akses yang tepat.

Back-up dan Recovery: Penting untuk memiliki kebijakan back-up data yang baik dan rencana pemulihan bencana untuk memastikan ketersediaan data rekam medis dalam situasi darurat seperti kegagalan perangkat keras atau bencana alam.

Maintenance dan *Monitoring*: Sistem harus dipelihara secara teratur dan dimonitor untuk memastikan ketersediaan yang optimal. Hal ini mencakup pemantauan kinerja sistem, peningkatan keamanan, dan perbaikan bug atau masalah teknis lainnya.

Kesesuaian Regulasi: Pastikan sistem RME memenuhi persyaratan regulasi dan kepatuhan data yang berlaku untuk menjaga ketersediaan data yang sah dan aman.

5. Aspek Kontrol Akses

Berdasarkan wawancara pada aspek kontrol akses, Salah satu komponen yang menyoroti prosedur dan metode yang harus diikuti untuk mengendalikan akses informasi adalah pengendalian akses.

Tabel 4. 5 Wawancara Kontrol Akses

Sub kategori	Pertanyaan	Hasil Wawancara Informan
Aspek Ketersediaan	"Siapa yang bertanggung jawab atas pengelolaan dan penerapan kontrol akses keamanan data dalam SIMRS dirumah sakit?"	*"untuk kontrol dan tanggung jawab sih dari IT ya, karna dari kita yang punya hak akses untuk memantau pengguna ya jadi ya dari IT"* Kepala IT
	"Bagaimana SIMRS memastikan bahwa akses ke data pasien dibatasi sesuai dengan prinsip kebutuhan, terutama untuk mengurangi risiko akses tidak sah?"	*"karna dari hak akses tadi kan ada kaya apa...apa ya namanya itu...kaya...ya nanti kalo unit ini ya bisa dibuka unit ini, bahkan satu unit pun nanti bisa berbeda kan ada level-level manajemen nya kaya staff, nanti kepala unit itu untuk tampilan SIMRS nya pun beda udah dipisah seperti itu, jadi memang kalo untuk yang nanti hak akses yang kaya data pasien yang penting itu nanti mungkin kepala unit yang bisa tapi kalo untuk sekedar laporan-laporan nanti mungkin staff nya yang bisa"*jawabnya. Kepala Staff
	"Mekanisme kontrol akses apa yang digunakan untuk mengontrol akses pengguna ke data pasien?"	*"selama ini kami juga rasanya belum melakukan kontrol itu mba jadi hanya sebatas memberikan hak akses aja setelah itu sepertinya kalo kontrol data pasien lebih ke IT,sama pendfataran kami belum pernah melakukan kontrol itu"*

		Kepala SDM

Dalam hal tersebut pada aspek Kontrol akses sudah terlaksana dengan baik, Aspek kontrol akses dalam pelaksanaan rekam medik elektronik pada sarana kesehatan sangat penting dalam menjaga kerahasiaan dan keamanan data medis pasien, ada beberapa analisis kontrol akses tersebut dengan identifikasi Pengguna, Sistem RME harus memiliki mekanisme yang kuat untuk mengidentifikasi setiap pengguna yang mengaksesnya, seperti login dengan username dan password, atau penggunaan teknologi identifikasi ganda (misalnya, token atau otentikasi dua faktor). Pengaturan Hak Akses, Setiap pengguna di fasilitas kesehatan harus memiliki hak akses yang sesuai dengan perannya. Misalnya, dokter harus memiliki akses penuh untuk melihat dan mengubah rekam medis pasien yang mereka tangani, sementara staf administrasi mungkin hanya membutuhkan akses terbatas untuk informasi administratif. Pengendalian Terhadap Akses, Sistem harus dilengkapi dengan mekanisme pengendalian akses yang memungkinkan administrator untuk mengatur dan mengelola hak akses secara efektif. Ini dapat mencakup pembatasan akses berdasarkan waktu tertentu atau lokasi fisik tertentu.

6. Aspek Nir-Sangkal

Berdasarkan hasil wawancara, Unsur ini mempunyai hubungan yang erat sama transaksi atapun pemutakhiran informasi. Fitur ini membantu mengatasi pengunggahan informasi yang mengindikasikan adanya transaksi atau modifikasi.

Tabel 4. 6 Wawancara Aspek Nir Sangkal

Sub kategori	Pertanyaan	Hasil Wawancara Informan
Aspek Nir sangkal	"Bagaimana SIMRS memastikan integrasi data, sehingga data pasien tetap akurat, lengkap, dan tidak dimanipulasi?"	*"untuk integrasi data itu tadi sebenarnya kita ada pebanding kaya nanti data pasien ini dia transaksi di kasir nah kita bandingkan juga data di kasir kemudian kita banding kan juga data di farmasi data di radiologi nah itu kan bisa diliat nanti kalo ada perbedaan data gitu*

		keliatan nanti ohh ini kok data beda sama yang dikasir ohh ini data beda sama yang farmasi terus kita konfirmasi ke unit yang bersangkutan yang bener kaya gini mas ohh ya nanti kita rubah kaya gitu" Kepala IT
	"Mekanisme non-repudiation apa yang digunakan untuk memastikan bahwa pengguna tidak dapat menyangkal tindakan mereka terkait perubahan atau penghapusan data pasien?"	*"nah itu kalo yang merubah kita masih belum bisa he eh belum ada tapi kalo penghapusan jelas bisa kelihatan"* Kepala SDM
	"Bagaimana hak akses diterapkan untuk mengontrol perubahan data pada SIMRS di rumah sakit Anda?"	*"eee...perubahan data? Kalo memang ada perubahan data kami menggunakan seperti surat eee...surat apa istilahanya surat kuasa, he eh Itu jadi kalo misal ada perubahan mereka harus mengajukan surat dulu ke kami nanti baru kami proses untuk pengajuan perubahan seperti itu, karna kalo tiba-tiba mengajukan perubahan khawatir kami nanti di belakang ada masalah kami yang kena gitu ya, jadi kemarin kesepakatan dengan Bu (kepala rekam medis) apapun perubahan itu kalo bisa hitam diatas putih jadi ada surat permohonannya sama seperti temen-temen misalnya yang eee...temen-temen mitra kerja baru sebelum kami berikan hak akses mereka harus mengisi dulu surat permohonan untuk permintaan hak akses kemudian menjaga raha- surat untuk menjaga rahasia (batuk) seperti itu. Karna takutnya adanya ya itu nanti dibelakang kok ada berubah, siapa yang ngerubah? Nah kan kan tapi kalo ada hitam diatas putih atau misalnya kita rapat gitu*

		ya ada perubahan itu eee...lebih enak gitu loh kita bisa baca notulennya kemudian ada eee...perjanjian nya itu kan lebih enak karna kadang disini minta dirubah nanti kemudian hari lupa gitu loh mbak jadi nya lebih aman seperti itu toh, karna kalo kami yang menyoroti karna saya dibagian SDM itu biasanya kan yang paling sering saya lihat itu pergantian jadwal, jadwal dokter. Nah itu kan sering sekali berubah jadi kadang tu kalo ada, ada perubahan di harapkan kami juga ada laporan bahwa dokter itu merubah kuota merubah jam, karna kadang-kadang berubah ga ada yang ngaku gitu toh jadi kesulitannya disitu, memang di SIMRS bisa langsung berubah Cuma siapa yang merubah kenapa alur nya itu yang kadang temen-temen pelaksana itu asal njawab yaa itu yang kami khawatir kan dibagian manajemen sehingga memang kesepakatan sama Mba (kepala rekam medis) kalo bisa perubah setiap perubahan itu harus ada bukti gitu, termasuk kalo- karna kalo di SIMRS itu merubah kan sebenarnya tidak tau kita- kita ga tau siapa sih yang merubah kecuali menghapus kalo menghapus di SIMRS emang kelihatan ohh sih A yang menghapus sih B yang menghapus tapi kalo merubah itu seperti nya masih belum bisa terbaca gitu" Kepala SDM

Dalam hal tersebut pada aspek Nir-Sangkal masih perlu adanya pembelajaran agar menciptakan keamanan dan kerahasiaan data pasien. Sehingga dapat memperhatikan Konsep "Nir Sangkal akses" dalam konteks

penerapan rekam medik elektronik (RME) di fasilitas kesehatan mengacu pada prinsip bahwa setiap akses atau tindakan yang tercatat dalam sistem harus dapat diidentifikasi kembali ke pengguna yang melakukan aksi tersebut. Ini berhubungan erat dengan audit trail dan keamanan sistem secara umum.

Pada audit Trail terkait dalam melakukan perubahan data di RSU Rajawali Citra pada SIMRS masih harus terus dikaji lebih mendalam demi mempertimbangkan pihak siapa saja yang terlibat dalam melakukan perubahan dapat di *Tracking* sebagai bentuk dari pengakuan atas perubahan yang dilakukan pihak terkait. Dijelaskan juga bahwa terkadang pihak-pihak yang melakukan perubahan tidak mengaku atas perubahan yang dilakukan yang dimana jika hal ini jika tidak cepat ditindak maka akan terjadi kerugian bagi petugas itu sendiri maupun bagi institusi kesehatan tempatnya bekerja. Tindakan itu juga merupakan pelanggaran terhadap kode etik profesi kesehatan. Kejujuran dan integritas nilai-nilai fundamental dalam profesi kesehatan, dan menyembunyikan perubahan data adalah bentuk ketidakjujuran.

7. Mengetahui Regulasi dan prosedur yang mengatur tentang keamanan data pada SIMRS RSU Rajawali Citra

Menurut hasil wawancara serta studi dokumentasi yang dikerjakan ketika penelitian, ditinjau ada regulasi mencakup kebijakan serta tahapannya. Hal ini hasil dokumentasi yang sudah peneliti kerjakan:

Tabel 4. 7 Hasil Studi Dokumentasi mengenai Regulasi

No	Dokumen	Ada		Keterangan
		Iya	Tidak	
1.	Kebijakan dalam perubahan password/kata sandi	✓		Keputusan Direktur Nomor 201.601.10 Backup DB dan pengamanan SIMRS
2.	kebijakan dan prosedur pengaturan kontrol akses keamanan untuk menjaga kerahasiaan data di SIMRS	✓		Keputusan Direktur Nomor 201.601.10 Backup DB dan pengamanan SIMRS
3.	kebijakan mengenai	✓		Keputusan Direktur Nomor

penggunaan SIMRS	201.601.002 Penggunaan SIMRS	Petunjuk	

B. Pembahasan

1. Karakteristik Informan Berdasarkan

Berdasarkan kriteria, pendidikan petugas minimal Diploma III, pengguna SIMRS selama lebih dari 1 tahun, petugas yang bersedia diwawancarai. Didapatkan informasi petugas sebagai berikut:

Tabel 4. 8 Informasi Petugas

Unit Kerja	Pendidikan	Jumlah	Masa Kerja	Jumlah
Rekam medis	S1	3	0-5 Tahun	4
	D-III	9	6-10 Tahun	5
	SMA	2	11-15 Tahun	4
		1	16-20 Tahun	2
	Total	15		15

Tabel 4. 9 Informasi Petugas

Unit Kerja	Pendidikan	Jumlah	Masa Kerja	Jumlah
IT	S1	2	20-25 Tahun	1
	S2	1	36-40 Tahun T	2
	Total	3		3

Tabel 4. 10 informasi Petugas

Unit Kerja	Pendidikan	Jumlah	Masa Kerja	Jumlah
SDM	SMA	58	0-6 Tahun	110
	D-I	4	6-11 Tahun	64
	D-III	105	11-16 Tahun	49
	S1	21	17-21 Tahun	23
	S1 Profesi	40	21-27 Tahun	10
	Spesialis	20		
	S2	8		
	Total	256		256

2. Kerahasiaan dan keamanan data pada sistem informasi dari aspek kerahasiaan

Kerahasiaan dan keamanan data yang dimiliki oleh RSU Rajawali Citra 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 atamemasukan username dan password. Untuk menghindari agar sistem tidak diakses oleh pengguna yang tidak memiliki wewenang, maka harus dikontrol dengan mengkombinasikan kontrol preventif dan pendeteksian.

Informasi dilindungi dari mereka yang tidak mempunyai hak hukum dalam mengaksesnya melalui privasi atau kerahasiaan. Data rekam medis yang disimpan serta disebarluaskan dengan cara elektronik hendak rentan terhadap penyalahgunaan, yang bisa membahayakan pasien. Data dari rekam medis pasien wajib dipastikan aman baik dari segi privasi ataupun keamanannya. Melalui prosedur pengelolaan data pasien yang dimulai berdasarkan tahapan pengumpulan data dan dilanjutkan dengan mutu data dan pengendalian akses, unsur privasi menjaga data rekam medis (Sofia et al., 2022).

Pada penelitian (Rijal Husni, 2022) mengatakan bahwa petugas yang mempunyai hak melakukan akses informed consent elektronik ialah petugas yang dikasih hak akses pada aplikasi sama admin, penetapan hak akses pengguna sistem pada informed consent elektronik dikerjakan sama tim IT selaras pada unit yang memberikan layanan informed consent, dia dikasih username serta password, pengguna bisa masuk pada sistem lewat metode input pada modul RME pada SIMRS lewat pengaksesan menu informed consent.

3. **kerahasiaan dan keamanan data pada sistem informas dari aspek integrasi**

Pada penelitian (Pradita et al., 2022) menyatakan bahwa Untuk menjamin input data kegiatan PKM berfungsi dengan baik, materi sosialisasi diberikan kepada petugas Instalasi Rekam Medis yang bertindak selaku pengguna. Berdasarkan informasi yang diberikan, rekam

medis elektronik menjamin keakuratan data dan informasi yang dikandungnya, serta cuma mereka yang mempunyai hak akses yang diperlukan yang bisa mengerjakan perubahan sama data itu. Untuk memastikan bahwa data pasien yang tercatat tidak dapat diubah oleh siapa pun selain pemilik informasi, rekam medis elektronik di e-Puskesmas harus dibuat dengan menggunakan teknik paling efektif yang ada Informasi sangat penting sehingga harus dilindungi agar tetap validitasnya.

Kebenaran data serta informasi yang terdapat pada rekam medis elektronik dijamin integritasnya, serta cuma mereka yang mempunyai hak akses yang bisa membuat perubahan pada data itu (Permenkes, 2022).

4. Kerahasiaan dan keamanan data pada sistem informasi dari aspek autentikasi

Autentikasi keamanan Sistem Informasi Rawat Jalan tidak mampu mengidentifikasi pengguna pada sistem, maka menggunakannya saja tidak cukup untuk mengautentikasi sistem keamanan. Satu-satunya cara pengguna dapat mengakses sistem adalah melalui otentikasi aman. Sementara itu, autentikasi perlu menjadi diantara komponen yang juga berperan penting pada menjaga data pada Sistem Informasi Klinik Rawat Jalan. Meskipun setiap agen pada dasarnya sudah memiliki password, namun hal ini tidak menjamin sistem keamanan akan berfungsi sebagaimana mestinya. Oleh karena itu, autentikasi diperlukan untuk mengidentifikasi dan mengotorisasi pengguna untuk memberi tahu mereka yang tidak peduli tentang keamanan sistem komputer sesegera mungkin. Jika otentikasi sesuai, hal ini akan membantu menjaga keamanan data klinik (Wiranata et al., 2023).

Penggunaan tanda tangan digital, atau tangan digital, pada transaksi elektronik mempunyai fungsi selaku sarana verifikasi dan identifikasi identitas. Tanda tangan elektronik, integritas data, dan validitas. Legalisasi dokumen elektronik merupakan salah satu penerapan tanda tangan digital. Pusat sertifikasi mendefinisikan tanda tangan digital selaku tanda tangan elektronik yang dipakai dalam memverifikasi identitas

pengirim dan keabsahan komunikasi ataupun dokumen (ditanda tangani sama tangan elektronik bersertifikat) (Abraham, 2019).

5. **Kerahasiaan dan keamanan data pada sistem informasi dari aspek ketersediaan**

Ketersediaan data dalam konteks keamanan dan kerahasiaan sistem informasi sangat penting untuk dipertimbangkan dalam buku yang di tulis oleh (Khristianto, 2022) menyampaikan bahwa Ketersediaan data dapat ditingkatkan dengan memanfaatkan teknologi redundansi, seperti RAID (*Redundant Array of Independent Disks*) untuk server penyimpanan data. Akses ke data dapat diakses bahkan jika satu atau lebih drive gagal berkat sistem ini. Memanfaatkan penyeimbangan beban atau pengelompokan, dua fitur arsitektur yang ditujukan untuk ketersediaan tinggi. Hal ini memungkinkan sistem untuk berfungsi bahkan ketika beberapa komponennya gagal. Keamanan Fisik: Mencegah akses ilegal dan bencana alam merusak perangkat keras sebenarnya yang menyimpan data. Hal ini termasuk mengendalikan kelembaban dan suhu, membatasi akses, dan menggunakan ruang server yang aman. Keamanan Jaringan: Untuk menjaga data dari ancaman jaringan, gunakan firewall, enkripsi data, dan metode keamanan jaringan lainnya. Dengan mempertimbangkan dan mengimplementasikan aspek-aspek ini, organisasi dapat meningkatkan ketersediaan data mereka sambil tetap menjaga kerahasiaan dan keamanannya.

6. **Kerahasiaan dan keamanan data pada sistem informasi dari aspek kontrol akses**

Kontrol akses ialah diantara faktor penting dalam keamanan sistem informasi dalam memastikan kalau cuma pengguna yang sah yang memiliki akses yang sesuai terhadap data dan sumber daya sistem. Dalam (Matthew Kosinski, 2024) menyatakan bahwa adanya *Multi-factor Authentication* (MFA) berguna untuk Menambahkan lapisan keamanan dengan memerlukan lebih dari satu cara untuk memverifikasi identitas pengguna, seperti kode yang dikirimkan ke perangkat seluler atau token

keamanan. Pengguna sering kali harus melalui proses autentikasi untuk mengakses sistem dan aset sensitif, seperti aplikasi perbankan, database pribadi, atau bahkan gedung perkantoran yang dibatasi. Oleh karena itu, mereka harus menunjukkan bahwa mereka adalah pengguna yang sah.

Dalam penelitian (Hariyadi & Prakasa, 2023) mengatakan bahwa perlu adanya *Access Control Policies* yang berguna untuk Kebijakan yang ditetapkan oleh organisasi untuk mengatur bagaimana kontrol akses diterapkan dalam sistem mereka, termasuk prosedur untuk mengelola hak akses dan sanksi untuk pelanggaran keamanan.

7. **Kerahasiaan dan keamanan data pada sistem informasi dari aspek nir-sangkal (*Non-Repudiation*)**

Pada Aspek ini seperti kita ketahui bahwa, Nir sangkal adalah Verifikasi penanda tangan dan surat-surat untuk keasliannya sebagai tindakan pencegahan dan penerapan gagasan tersebut "*non repudiation*" dalam informasi yang berkaitan dengan sektor keamanan. *Non repudiation* adalah jaminan keaslian atau penyerahan surat asli untuk mencegah penolakan baik dari pengirim maupun penandatangan, yang mungkin menyatakan bahwa mereka tidak mengirimkan dokumen atau tidak menandatanganinya (Lapian et al., 2024).

Faktor Nir sangkal bisa didorong lewat kriptografi lewat penggunaan algoritma tanda tangan digital. Mekanisme penggunaan algoritma ini sama semisal mekanisme dalam otentikasi. Individu yang sudah mengirimkan pesan serta dibubuhi digital signature tidak bisa mengelak alau dia sudah mengirimkan pesan sebab digital signature itu didapatkan dari enkripsi nilai hash pesan atas kunci privatnya (Aria et al., 2023).

C. Keterbatasan Penelitian

Beberapa faktor yang menjadi keterbatasan dalam penelitian ini yang menjadikan penelitian belum mencapai tahap sempurna:

1. Waktu Penelitian: dengan waktunya yang tersedia menyebabkan penelitian ini dilakukan dengan terburu-buru untuk mengejar target yang ada.
2. Instrumen Penelitian: dengan adanya kendala yang didapatkan peneliti selama pengambilan data pada informan, didapati beberapa informan yang kurang dalam penyampaian informasi dan terkesan meleparkan pertanyaan, serta kurangnya responsif dari informan yang menyebabkan penelitian ini dapat dikatakan masih jauh dalam kata sempurna.