



ANALISIS PENGGANTIAN PASSWORD USER ID DALAM SISTEM REKAM MEDIS ELEKTRONIK GUNA MENJAGA KEAMANAN DATA REKAM MEDIS DI RUMAH SAKIT HERMINA ARCAMANIK

Oleh

Alia Rahma¹, Ade Irma Suryani²

^{1,2}Program Studi Rekam Medis dan Informasi Kesehatan
Politeknik Piksi Ganesha

Jl.Jend. Gatot Soebroto No.301 Bandung.

e-mail: ¹alياهو55@gmail.com, ²adeirmasuryani20@gmail.com

Abstrak

Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 menetapkan bahwa rekam medis elektronik harus aman dan dijamin rahasianya. Tujuan dari penelitian ini adalah untuk menilai tingkat keamanan rekam medis elektronik dan data di RS Hermina Arcamanik. Metode penelitian kualitatif deskriptif digunakan untuk memberikan gambaran mendalam tentang bagaimana rumah sakit mengelola dan melindungi rekam medis mereka. Teknik pengumpulan data observasi dan wawancara. Seiring dengan meningkatnya penggunaan catatan kesehatan elektronik dalam layanan kesehatan, memastikan keamanan dan kerahasiaan data pasien menjadi hal yang penting. Hal ini sangat penting terutama dalam hal otentikasi pengguna dan kontrol akses dalam sistem rekam medis elektronik. Penelitian ini fokus pada penerapan penggantian user ID sebagai langkah pengamanan pada sistem rekam medis elektronik yang bertujuan untuk menjaga integritas dan kerahasiaan data pasien. Studi ini menyelidiki kelemahan dalam sistem manajemen identitas pengguna saat ini, termasuk kurangnya sistem identifikasi yang kuat dan rendahnya kesadaran akan konsep tersebut di kalangan staf medis. Untuk mengatasi masalah ini, penelitian ini menyarankan untuk memperkenalkan penggantian ID pengguna sebagai solusi. Hal ini termasuk mengubah ID pengguna secara berkala untuk meminimalkan risiko akses tidak sah dan penipuan identitas. Dengan mengubah ID pengguna, organisasi layanan kesehatan dapat meningkatkan keamanan sistem rekam medis elektronik mereka dan melindungi data pasien dari akses yang tidak sah. Untuk meningkatkan kesadaran pengguna terhadap keamanan data, khususnya sosialisasi tentang konsekuensi pertukaran nama pengguna dan kata sandi dengan orang lain dan kewajiban untuk mengubah kata sandi secara berkala, minimal 1 bulan sekali, dan pemasangan rekam medis dan penanggung jawab persetujuan melaksanakan tugas pengawasan pelaksanaan rekam medis elektronik sehari-hari.

Kata Kunci: Penggantian Password User Id, Keamanan, Rekam Medis

PENDAHULUAN

Peraturan Menteri Kesehatan No. 3 Tahun 2020 mendefinisikan rumah sakit sebagai institusi pelayanan kesehatan yang memberikan layanan kesehatan secara menyeluruh kepada individu, termasuk rawat inap, rawat jalan, dan layanan gawat darurat. Rumah sakit berfungsi sebagai pusat perawatan yang menawarkan berbagai jenis perawatan

medis dan kesehatan untuk memenuhi kebutuhan pasien secara menyeluruh. Sementara itu, menurut World Health Organization (WHO) pada tahun 1957, Rumah Sakit adalah bagian dari organisasi medis dan sosial yang bertanggung jawab untuk memberikan layanan kesehatan yang luas kepada masyarakat, termasuk pengobatan dan pencegahan. Layanan ini juga mencakup



keluarga dan lingkungan sekitar. Rumah Sakit juga berfungsi sebagai tempat pelatihan tenaga medis dan penelitian biologi, psikologi, sosial ekonomi, dan budaya.

Rekam medis menurut Permenkes RI No. 24 Tahun 2022, adalah dokumen yang berisi informasi tentang identitas pasien, pemeriksaan, pengobatan, tindakan, dan layanan yang diberikan kepada pasien. Rekam medis elektronik adalah rekam medis yang dibuat menggunakan sistem elektronik untuk mengelola data medis. Semua petugas kesehatan yang bekerja di fasilitas kesehatan memiliki tanggung jawab untuk memastikan bahwa rekam medis tetap aman dan rahasia.

Rekam medis harus diselenggarakan secara digital karena perkembangan teknologi digital di masyarakat yang mendorong digitalisasi layanan kesehatan. Yang mana berarti rekam medis harus diselenggarakan secara elektronik dengan prinsip keamanan dan kerahasiaan data dan informasi. Meskipun ada kemudahan dan keuntungan dari penggunaan rekam medis elektronik, ada juga risiko yang harus diperhatikan oleh setiap fasilitas pelayanan kesehatan (Ramadhanti, 2022). Keamanan data adalah salah satu masalah utama yang terkait dengan kemajuan teknologi informasi saat ini.

Rekam medis elektronik, menurut PMK No. 24 Tahun 2022, adalah rekam medis yang dibuat menggunakan sistem elektronik untuk mengelola rekam medis. Rekaman medis elektronik membantu manajemen rumah sakit mencatat informasi penting seperti kunjungan dokter dan keakuratan perawatan, sehingga menghemat waktu, biaya, dan mencegah duplikat data. Dengan demikian, rekam medis elektronik memungkinkan tenaga kesehatan memberikan pelayanan yang lebih baik kepada pasien dan mengurangi risiko kesalahan medis (Soraya et al., 2022).

Keamanan data berarti memastikan bahwa data dalam sistem tidak dapat dilihat atau diubah oleh orang-orang yang tidak berwenang (Aditya, 2021). Semua pemilik dan

pengelola sistem informasi harus memastikan bahwa data yang disimpan aman dan hanya dapat diakses oleh pihak yang berwenang. Tujuan dari langkah ini adalah untuk melindungi data dari serangan yang disengaja maupun tidak disengaja. Keamanan data, yang mencakup kerahasiaan, integritas, dan ketersediaan, adalah tanggung jawab rumah sakit yang mengelola rekam medis elektronik. Keselamatan dan kepercayaan pasien dapat dipertahankan dengan penerapan kebijakan keamanan yang menyeluruh. Untuk mendukung layanan kesehatan yang aman dan terpercaya, kebijakan ini harus mempertimbangkan kerahasiaan, integritas, dan ketersediaan data, terutama dalam kasus pelanggaran data (Kementerian Kesehatan Republik Indonesia, 2022). Melindungi informasi dari pihak yang tidak berhak mengaksesnya adalah bagian penting dari kerahasiaan, menurut Nugraheni & Nurhayati (2018). Otentikasi mengacu pada pengendalian akses ke informasi, sedangkan integritas memastikan bahwa informasi tidak diubah tanpa izin. Rumah Sakit Hermina Arcamanik menggunakan RME sebagai bagian penting dari sistem informasi kesehatannya. Keamanan RME sangat penting karena menyimpan data pasien yang sensitif dan rahasia. Melakukan penggantian password user ID secara berkala adalah salah satu cara untuk menjaga keamanan RME.

Tiorentap dan Hosizah (2020) menemukan bahwa prinsip keamanan sistem informasi di klinik pengawasan medis tidak konsisten. Mereka menemukan bahwa banyak orang menggunakan user ID dan password yang sama untuk bertukar data, dan bahwa banyak orang menggunakan lebih dari satu user ID. Praktik ini bertentangan dengan prinsip kontrol akses yang berfokus pada membatasi hak orang untuk mengakses informasi. Jika terjadi kesalahan penginputan data, konsekuensinya bisa sangat serius dan akan mempersulit proses identifikasi pelaku. Ini sangat mengkhawatirkan karena hal ini dapat



memungkinkan pihak-pihak yang tidak bertanggung jawab untuk menggunakan data.

Merujuk pada penelitian tersebut, ditemukan hasil bahwa fitur kerahasiaan, seperti kemampuan login dengan username dan password, logout otomatis, dan kemampuan untuk mengganti password secara berkala, sudah tersedia, tetapi pengoperasiannya masih kurang optimal dari perspektif pengguna. Hal ini karena ada petugas yang masih menggunakan user ID yang dimiliki oleh petugas lain. Selama beberapa dekade terakhir, pakar keamanan siber telah menyarankan agar pengguna internet mengubah password mereka setiap dua hingga tiga bulan untuk meningkatkan keamanan data. Di rumah sakit, protokol penggantian password secara berkala harus diperkuat dengan instruksi dan pengawasan yang ketat untuk memastikan setiap petugas mematuhi protokol keamanan yang telah ditetapkan.

Mengganti password dan informasi kredensial lainnya, seperti pin dan passcode, secara teratur adalah untuk mencegah orang lain dapat menggunakan informasi kredensial yang hilang, dicuri, atau dipalsukan. Fungsi dari penggantian password untuk melindungi data dan informasi penting akun. Kerugian tidak melakukan penggantian password bisa menimbulkan kesalahan dalam melakukan upload berkas Rekam Medis pasien. Kerugian lainnya yaitu petugas sering adanya kesalahan dalam transaksi dikarenakan masih terdapat petugas yang masih memakai user id petugas yang lain.

Penelitian sebelumnya telah menekankan pentingnya penggantian password user id pengguna untuk menjaga keamanan data rekam medis, namun juga memerlukan pelatihan pengguna, teknik keamanan tambahan, dan adaptasi terhadap situasi penggunaan tertentu.

LANDASAN TEORI

2.1 Rekam Medis Elektronik

Rekam medis adalah kumpulan catatan dan dokumen yang berisi informasi lengkap

tentang identitas pasien, pemeriksaan, pengobatan, prosedur, dan layanan lainnya yang diberikan kepada pasien. Rekam medis juga mencakup catatan yang dibuat di fasilitas medis dan merupakan bagian penting dari pelayanan kesehatan. Dokumen ini sangat penting untuk memastikan bahwa setiap aspek perawatan pasien tercatat dengan baik, sehingga informasi yang lengkap dan akurat tersedia untuk pasien.

Data yang lengkap dari rekam medis dapat membantu orang membuat keputusan tentang perawatan, intervensi medis, dan aspek lainnya. Setiap rekam medis wajib dilengkapi oleh dokter atau dokter gigi sesuai dengan ketentuan yang berlaku.

2.2 Keamanan Data

Keamanan data adalah proses menjaga kerahasiaan, integritas, dan ketersediaan data organisasi dengan cara yang konsisten dengan strategi risiko organisasi.

2.3 User ID

User Id adalah kode unik atau nomor identifikasi yang diberikan sistem kepada setiap pengguna terdaftar. User Id bersifat internal dan tidak selalu terlihat oleh pengguna lain kecuali memiliki alasan atau preferensi tertentu. User Id digunakan oleh sistem untuk mengidentifikasi secara unik setiap pengguna di database atau di lingkungan sistem tertentu.

METODE PENELITIAN

Penelitian adalah metode ilmiah yang digunakan untuk mengumpulkan data untuk memahami fenomena atau mencapai tujuan tertentu. Pendekatan ini mencakup berbagai teknik dan prosedur yang digunakan untuk mendapatkan informasi yang relevan dan akurat yang dapat digunakan untuk menganalisis, mengevaluasi, dan menarik kesimpulan tentang subjek penelitian. Dalam penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif. Metode kualitatif adalah pendekatan penelitian di mana peneliti secara langsung menyelidiki sumber data atau responden berdasarkan temuan



lapangan. Sampel yang diambil dalam penelitian ini melibatkan penggantian password user ID sebanyak 18 kali selama periode Januari hingga Maret.

Teknik pengumpulan data yang digunakan dalam penelitian ini diperoleh melalui observasi dan wawancara dengan berbagai narasumber. Wawancara dilakukan dengan kepala ruangan dengan mengajukan 7 pertanyaan untuk memperoleh pengumpulan data. Wawancara ini diberikan kepada petugas rekam medis yang sedang dilakukan penelitian di RSU Hermina Arcamanik.

HASIL DAN PEMBAHASAN

Rekam Medis Elektronik merupakan salah satu elemen penting dalam pengelolaan data pasien di RS Hermina Arcamanik (Rahma & Mayesti 2019). Hal ini karena sistem Rekam Medis elektronik memungkinkan penyimpanan dan akses data yang lebih efektif dan efisien. Namun keamanan data dalam sistem pencatatan pasien elektronik juga penting. Salah satu langkah yang dapat dilakukan untuk menjamin keamanan data Rekam Medis RS Hermina Arcamanik adalah dengan mengganti password user ID secara berkala. Ada beberapa alasan untuk mengubah User ID pengguna secara berkala, yang menegaskan pentingnya praktik ini dalam menjaga keamanan data Rekam Medis. Pencegahan akses penggunaan Rekam Medis tanpa izin dilaksanakan dengan bentuk kertas maupun elektronik, bentuk kertas menetapkan area penyimpanan terbatas (petugas dapat mengakses menggunakan door lock akses serta rambu area terbatas), bentuk elektronik dilindungi dengan penggunaan user id dan password. Instrumen Pengumpulan Data Instrumen penelitian yang digunakan pada penelitian ini adalah wawancara. Wawancara berupa daftar pertanyaan yang terdiri dari 7 pertanyaan kebijakan penggantian password user id. wawancara ini diberikan kepada petugas rekam medis yang sedang dilakukan penelitian di RSU Hermina Arcamanik. Pertanyaan yang diajukan kepada petugas

rekam medis berkaitan dengan faktor faktor yang mempengaruhi kepatuhan pengguna terhadap kebijakan penggantian password user id, kebijakan penggantian password user id efektif dalam menjaga keamanan data Rekam Medis, kebijakan penggantian password user id di RS Hermina Arcamanik, pergantian user id itudiakibatkan oleh apa, langkah langkah yang perlu dilakukan setelah mengganti password untuk memastikan keamanan akun.

Keamanan data rekam medis sangat penting untuk melindungi privasi pasien dan mencegah penyalahgunaan data. Berbagai ancaman keamanan data rekam medis, seperti akses tidak sah, peretasan, dan pencurian data, dapat membahayakan pasien dan merusak reputasi rumah sakit. kebijakan penggantian password user id sangat efektif dalam menjaga keamanan data Rekam Medis. Dengan mengubah password secara berkala, risiko akses tidak sah oleh pihak yang telah mendapatkan password lama dapat diminimalisir. Dalam kasus kebocoran data, kebijakan ini dapat membantu mengurangi dampak negatif, karena password yang bocor akan segera menjadi tidak valid setelah periode perubahan. Kepatuhan pengguna terhadap kebijakan penggantian password user ID dipengaruhi oleh berbagai faktor, seperti kesadaran keamanan, kemudahan penggunaan kebijakan, sanksi pelanggaran, human eror, ketertiban, SDM, dan mengundang kriminalitas. Pergantian user ID dalam beberapa bulan terakhir dapat disebabkan oleh berbagai faktor, yang umumnya berkaitan dengan upaya meningkatkan keamanan dan respons terhadap insiden keamanan. Faktor yang mengakibatkan pergantian user id selama beberapa bulan ini diakibatkan dari SDM yang terlalu banyak beban kerja akhirnya disaat pergantian shift SDM tersebut lupa untuk logout dari user ID mereka, hal ini dapat menimbulkan risiko keamanan yang serius, terutama dalam konteks data rekam medis yang sangat sensitif. Dengan menggabungkan solusi teknologi dengan edukasi dan kebijakan yang



ketat, organisasi dapat secara signifikan mengurangi risiko yang disebabkan oleh kelalaian logout oleh SDM. Terlalu banyak petugas dalam satu shift bisa menyebabkan salah transaksi dikarenakan petugas lain masih menggunakan user id yang sebelumnya digunakan oleh petugas yang masih memakai user id tersebut. Sebelum batas waktu yang ditentukan, sistem akan secara otomatis memberi tahu pengguna bahwa mereka harus mengubah kata sandi. Pemberitahuan ini akan dikirimkan beberapa hari sebelum tanggal jatuh tempo, sehingga pengguna memiliki waktu yang cukup untuk mengubah kata sandi dengan nyaman. Hal ini bertujuan untuk memastikan bahwa keamanan dan kerahasiaan data tetap terjaga. Pengguna harus login ke sistem menggunakan user ID dan password yang valid saat ini. Pengguna akan diminta memasukkan kata sandi yang sedang mereka gunakan. Pengguna harus memasukkan kata sandi baru. Kata sandi biasanya harus memenuhi persyaratan tertentu, seperti: Panjang karakter minimal, kombinasi huruf besar dan kecil, angka, dan simbol. Pengguna akan diminta memasukkan kembali kata sandi baru untuk menghindari kesalahan ketik.

Privasi atau kerahasiaan mengacu pada perlindungan informasi dari pihak yang tidak berwenang. Penyalahgunaan data medis yang disimpan dan didistribusikan secara elektronik sangat berbahaya bagi pasien. Oleh karena itu, privasi dan keamanan harus memastikan bahwa catatan pasien aman. Perlindungan data mencakup pengelolaan data pasien melalui berbagai proses pengumpulan, menjaga kualitas data, dan mengontrol akses ke data. Menurut artikel yang telah diteliti, organisasi layanan kesehatan harus mengambil sejumlah tindakan penting untuk melindungi rekam medis mereka. Proses ini mencakup penggunaan enkripsi untuk menjaga kerahasiaan data, penerapan metode logout otomatis, dan login dengan nama pengguna dan kata sandi. Data juga menunjukkan bahwa mereka juga menggunakan metode canggih,

seperti memblokir data melalui teknologi jaringan. Tinjauan terhadap artikel yang ditemukan menemukan bahwa sebagian besar artikel, membahas penerapan keamanan rekam kesehatan elektronik, dengan menerapkan login nama pengguna dan kata sandi. Nama pengguna dan kata sandi digunakan untuk menyatakan bahwa pengguna berwenang untuk menggunakan dan memasuki sistem. Oleh karena itu, sebelum dapat mengakses sistem informasi, semua pengguna harus memasukkan username dan password mereka. Sebuah kombinasi kontrol pencegahan dan deteksi diperlukan untuk mencegah akses oleh pengguna yang tidak sah. Mekanisme login menggunakan username dan password memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses informasi, meningkatkan keamanan data dan mencegah potensi pelanggaran. Ini adalah cara sistem informasi yang digunakan harus memastikan aspek perlindungan data. Keamanan informasi bukan hanya masalah teknis tetapi juga melibatkan sumber daya manusia. Karena fakta bahwa mereka memiliki sumber daya teknologi, mereka merupakan salah satu ancaman terbesar bagi keamanan berbagai bidang, termasuk kesehatan. Sebagian besar pelanggaran keamanan disebabkan oleh faktor manusia, seperti kelalaian atau kesalahan manusia biasa, yang dapat fatal bagi penyedia layanan kesehatan. Oleh karena itu, tidak hanya penting untuk menerapkan teknologi keamanan yang canggih, tetapi juga penting untuk meningkatkan kesadaran dan pelatihan keamanan bagi seluruh staf untuk mengurangi risiko kesalahan manusia. Menerapkan nama pengguna dan kata sandi saja tanpa mengedukasi pengguna tentang keamanan data tidaklah cukup untuk menjaga keamanan data pasien. Oleh karena itu, untuk melindungi informasi, perlu dipahami kesadaran keamanan pengguna sistem informasi. Untuk melindungi privasi data dan mengurangi pelanggaran dunia maya serta masalah keamanan informasi lainnya, sangat penting untuk memahami



keamanan data. Rekam medis seringkali disalahgunakan untuk tujuan non-medis karena banyak personel yang merawat pasien yang sama memiliki akses ke rekam medis elektronik. Akibatnya, risiko kehilangan data meningkat. Oleh karena itu, prosedur keamanan ketat perlu diterapkan untuk memastikan bahwa informasi medis hanya dapat diakses dan digunakan sesuai dengan tujuan medis yang sah. Sistem informasi juga harus memiliki fitur yang memungkinkan pengguna untuk secara otomatis keluar atau logout dari sistem jika tidak ada aktivitas dalam jangka waktu tertentu. Fitur ini sangat penting untuk mencegah pihak yang tidak berwenang mengakses sistem ketika pengguna meninggalkan komputer terlalu lama. Dengan mekanisme logout otomatis ini, risiko penyalahgunaan sistem informasi oleh orang yang tidak berwenang akan berkurang. Aspek perlindungan data ditunjukkan dengan bentuk tidak aktif (logout otomatis) sistem informasi jika tidak ada aktivitas oleh pengguna dalam waktu 5 menit. Ini berguna untuk melindungi atau mencegah penyalahgunaan user ID. Untuk memastikan bahwa data pasien yang tersimpan di rekam medis elektronik di fasilitas kesehatan aman, pertimbangan privasi diterapkan secara menyeluruh. Guna mencegah pihak-pihak yang tidak berwenang mengaksesnya, banyak organisasi kesehatan telah menerapkan kebijakan privasi yang ketat. Informasi yang disimpan dalam catatan kesehatan digital dilindungi dengan adanya langkah-langkah pencegahan ini. Pasien tidak lagi perlu khawatir bahwa pihak ketiga dapat mengakses data mereka tanpa izin mereka. Kebijakan ini meningkatkan kepercayaan pasien terhadap sistem kesehatan elektronik dan melindungi mereka.

PENUTUP

Kesimpulan

Mengganti password user id merupakan langkah efektif untuk menjaga keamanan data. Hal ini mengurangi resiko penggunaan password yang sudah diketahui oleh pihak yang

tidak berkepentingan. Kunci keberhasilan ini adalah meningkatkan kesadaran dan melatih seluruh staf Rumah Sakit akan pentingnya keamanan data dan kerahasiaan kata sandi. Terlalu banyaknya petugas dalam satu shift secara bergantian, sehingga satu pekerjaan dikerjakan banyak orang. Sumber daya manusia (SDM) sering lupa logout menggunakan id pengguna mereka, hal ini dapat menimbulkan berbagai masalah keamanan dan efisiensi dalam organisasi. Kunci keberhasilan ini adalah meningkatkan kesadaran dan melatih seluruh staf RS akan pentingnya keamanan data dan kerahasiaan kata sandi.

Saran

Memberikan pelatihan berkala kepada seluruh karyawan mengenai keamanan password dan pentingnya menjaga keamanan data Rekam Medis. Mendistribusikan materi pelatihan secara berkala untuk meningkatkan pengguna akan praktik keamanan yang baik.

DAFTAR PUSTAKA

- [1] Aditya, Y. S., Herdianto, U. Y. K. S., & Fathinuddin, M. (2021). Pengamanan Data Cloudfri Menggunakan Metode Security Hardening. *eProceedings of Engineering*, 8(5). <https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/15807>
- [2] Hidayah, E. N. (2023). *Analisis Aspek Keamanan Data Pada Hospital Information System (His) Dalam Penerapan Rekam Medis Elektronik Di Rsup Nasional Dr. Cipto Mangunkusumo Jakarta*.
- [3] Kementerian Kesehatan. (2020). *Peraturan Menteri Kesehatan Nomor 3 Tahun 2020 tentang Klasifikasi dan Perizinan Rumah Sakit*.
- [4] Kementerian Kesehatan. (2022). *Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis (BN.2022/No.829)*.



-
- [5] Kementerian Kesehatan. (2022). Peraturan Menteri Kesehatan Republik Indonesia Nomor 30 Tahun 2022 tentang Indikator Nasional Mutu Pelayanan Kesehatan. *Peraturan Menteri Kesehatan Republik Indonesia*, 879.
- [6] Nugraheni, N. (2018). Aspek Hukum Rekam Medis Elektronik di RSUD Dr Moewardi. *Prosiding Seminar Nasional Unimus*, 1.
- [7] Rahma, N., & Mayesti, N. (2019). Pengendalian Hak Akses pada Electronic Document and Records Management System di Kementerian Kelautan dan Perikanan Republik Indonesia. *Lentera Pustaka: Jurnal Kajian Ilmu Perpustakaan, Informasi dan Kearsipan*, 5(1), 33. <https://doi.org/10.14710/lenpust.v5i1.23578>
- [8] Ramadhanti, A. T. (2022). *Analisis Aspek Keamanan Informasi Pasien dalam Penerapan Rekam Medis Elektronik di Rumah Sakit PHC Surabaya*.
- [9] 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>
- [10] 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*. ISBN: 978-623-6566-34-3, 4(0).



HALAMAN INI SENGAJA DIKOSONGKAN