Tinjauan Keamanan Data Rekam Medis Elektronik Pada Aplikasi Simpus Berdasarkan Aspek *Confidentiality*, *Integrity*, Dan *Availability* Di Puskesmas Tasikmadu Karanganyar

Overview of Electronic Medical Record Data Security In the Simpus Application Based on Confidentiality Aspects, Integrity and Availability at the Tasikmadu Karanganyar Community Health Center

Septiana Wahyu Widiyanti[1], Nunik Maya Hastuti[2], Erna Adita Kusumawati[3]

[1,2,3]STIKes Mitra Husada Karanganyar
Jl. Brigjen Katamso Barat, Gapura Papahan Indah, Papahan Kec. Tasikmadu, Kabupaten Karanganyar, Jawa Tengah 57722

Email : aseptiana738@gmail.com, nunikmaya21@gmail.com, ernaadita@gmail.com

Abstrak

Keamanan data merupakan terjaganya kerahasiaan, keutuhan, dan ketersediaan informasi. Keamana data pasien pada SIMPUS di Puskesmas Tasikmadu Karanganyar belum adanya *Automatic Log Off*. Hal itu dapat mengakibatkan sistem diakses oleh orang pengguna yang tidak berhak (otorisasi) dan dapat terjadinya kebocoran informasi. Tujuan penelitian ini untuk mengetahui keamanan data SIMPUS di Puskesmas Tasikmadu Karanganyar. Jenis penelitian yang digunakan adalah *deskriptif* dengan pendekatan *kualitatif*. Subyek dalam penelitian ini adalah pengguna SIMPUS bagian pendaftaran Rawat Jalan sedangkan objeknya adalah SIMPUS bagian pendaftaran Rawat Jalan. Cara pengumpulan data adalah wawancara dan observasi dengan menggunakan instrumen penelitian pedoman wawancara tidak terstruktur dan observasi. Teknik pengolahan adalah pengumpulan, *editing*, reduksi data, penyajian data, dan penarikan kesimpulan. Analisis yang digunakan adalah *deskriptif*. Hasil penelitian tinjauan keamanan data rekam medis elektronik pada aplikasi SIMPUS berdasarkan aspek *confidentiality*, *integrity*, dan *availability* di Puskesmas Tasikmadu Karanganyarn bahwa keamanan data pada aspek *confidentiality* dimana saat *log-in* ke aplikasi SIMPUS user sudah mempunyai hak *otentikasi* menggunakan *username* dan *password* disetiap bagiannya. Hanya saja SIMPUS belum dilengkapi dengan *Automatic Log Off*. Dibagian aspek *integrity* keamanan datanya sudah dikatakan aman karena data hanya bisa diedit oleh pengguna pelayanan dibagiannya saja dan untuk penghapusan data hanya bisa dilakukan oleh pihak berwenang, di bagian aspek *availability* dimana dalam aspek ini sudah menunjang untuk keamanan datanya dikarenakan saat data dibutuhkan pasti tersedia. Data SIMPUS juga bisa diakses dimanapun asalkan mempunyai hak akses. Untuk *back-up* datanya masih manual yang dilakukan setiap hari atau bisa di lakukan secara *periodic* jadi belom otomatis *back-up* data.

Kata Kunci **:** Keamanan Data SIMPUS, Confidentiality, Integrity, Availability

Abstract

Data security is the confidentiality, integrity, and availability of information. The security of patient data in SIMPUS at Puskesmas Tasikmadu Karanganyar does not yet have an Automatic Log Off. It can cause the system being accessed by unauthorized users and information leakage. The purpose of this study was to know the security of SIMPUS data at Puskesmas Tasikmadu Karanganyar. The type of research used was descriptive with qualitative approach. The subjects in this study were SIMPUS users in the outpatient registration section while the object is SIMPUS in the outpatient registration section. The data were collected through interview and observation by using research instruments i.e. unstructured interview guidelines and observation. the technique of data analysis covered, editing, data reduction, data

presentation, and conclusion drawing. The analysis used was descriptive. The results of the research showed that the security review of electronic medical record data in the SIMPUS application based on confidentiality, integrity, and availability at Puskesmas Tasikmadu Karanganyar stated that data security in the confidentiality aspect when the user logged in to the SIMPUS application the user had already has authentication rights using a username and password in each section. How ever, SIMPUS had not yet equipped with Automatic Log Off. In the integrity aspect, the data security was said to be safe because the data could only be edited by service users in their section only and for data deletion could only be done by author. In the availability aspect, it had this supported the data security because the data were always available when needed. SIMPUS data could also be accessed anywhere as long as it had access rights. The data back-up was manual which was done daily or periodically so the data back-up had not geen automatic yet.

Keywords: SIMPUS Data Security, Confidentiality, Integrity, Availability

PENDAHULUAN

Di Indonesia, penguatan peran sektor kesehatan merupakan pilar penting program pembangunan, selain sektor pendidikan. Dalam hal ini, penguatan peran puskesmas sebagai garda terdepan dalam pelayanan kesehatan masyarakat merupakan hal yang sangat penting dalam program kesehatan pemerintah. Salah satunya adalah memastikan ketersediaan data kesehatan masyarakat untuk mengukur kinerja dan mengembangkan kebijakan (Barsasella, 2012).

Dalam era digital pemanfaatan teknologi informasi tidak lagi menjadi nilai tambah namun sudah menjadi standar implementasi Sistem Informasi Manajemen Puskesmas (SIMPUS) yang merupakan solusi tepat untuk meningkatkan standar pelayanan kesehatan (Barsasella, 2012). Menurut Permenkes RI Nomor 31 Tahun 2019 Tentang Sistem Informasi Puskesmas menyatakan bahwa SIMPUS adalah suatu tatanan yang menyediakan informasi untuk membantu proses pengambilan keputusan dalam melaksanakan. Di sisi lain, menurut Qamaddin (2020), keamanan data adalah jaringan entitas yang berkomunikasi yang dapat dibuat dengan berbagai cara, seperti perutean, kebijakan kontrol akses atau yang mungkin termasuk pelabelan yang meliputi bagaimana sistem diberi label sehingga mampu mengekspresikan banyak jenis persyaratan keamanan.

Menurut Peraturan Arsip Nasional Republik Indonesia Nomor 15 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi di Lingkungan Arsip Nasional Indonesia, keamanan informasi berarti menjaga kerahasiaan, keutuhan, dan ketersediaan informasi. Hubungan antara SIMPUS dan keamanan sistem pada dasarnya sama dengan Sistem Informasi Manajemen Puskesmas menjamin kerahasiaan organisasi.

Berdasarkan Survey pendahuluan di Puskesmas Tasikmadu Karanganyar ditemukan bahwa keamanan data pasien pada SIMPUS belum adanya *Automatic Log Off*, dikarenakan saat sistem ditinggalkan oleh pengguna tidak dapat *Automatic Log Off*. Hal itu dapat mengakibatkan sistem diakses oleh pengguna yang tidak berhak dan dapat terjadinya kebocoran informasi. Maka dari itu, perlu adanya keamanan data pada aplikasi SIMPUS.

METODE PENELITIAN

Jenis penelitian ini adalah deskriptif dengan pendekatan kualitatif yaitu penelitian yang menggambarkan dan menganalisis tentang keamanan data rekam medis elektronik pada aplikasi SIMPUS berdasarkan aspek *confidentiality*, *integrity*, dan *availability* di Puskesmas Tasikmadu Karanganyar. Penelitian ini dilaksanakan di bagian pendaftaran Rekam Medis Rawat Jalan Puskesmas Tasikmadu Karanganyar. Penelitian dilakukan pada bulan Februari sampai Maret tahun 2024. Subyek dari penelitian merupakan 3 petugas pengguna SIMPUS yaitu petugas pendaftaran Rekam Medis, Perawat dan Kepala Rekam Medis. Penentuan subyek menggunakan *purposive sampling* berdasarkan rekomendasi. Kriteria dalam penentuan subyek penelitian ditentukan berdasarkan lamanya petugas yang sudah menggunakan SIMPUS minimal 1 tahun. Objek dalam penelitian ini adalah Aplikasi Sistem Informasi Manajemen Puskesmas (SIMPUS) bagian Rekam Medis Rawat Jalan Puskesmas Tasikmadu Karanganyar. Instrumen penelitian

terdiri dari pedoman observasi, pedoman wawancara, dan alat perekam. Cara pengumpulan data terdiri dari observasi dan wawancara tidak terstruktur. Teknik pengolahan data terdiri dari pengumpulan data, penyuntingan data, penyaringan data, penyajian data, dan penarikan kesimpulan. Analisis data yang digunakan dalam penelitian ini adalah analisis deskriptif.

HASIL DAN PEMBAHASAN

Keamanan Data SIMPUS di tinjau Berdasarkan Aspek Confidentiality

Berdasarkan hasil wawancara dan observasi dapat disimpulkan terkait hasil wawancara dan hasil observasi ditinjau dari aspek *Confidentiality* sebagai berikut:

a. Pengelolaan data otentikasi saat login ke SIMPUS setiap user bagian sudah mempunyai username dan password sendiri-sendiri. Jadi tidak semua orang bisa mengakses aplikasi SIMPUS menggunakan hak akses tidak sah (otorisasi)
b. Pengaksesan aplikasi SIMPUS bisa di akses lebih dari satu orang.
c. Penerapan dalam pembuatan password bebas belum kombinasi angka dan huruf, terkait kesalahan entry data menjadi tanggung jawab setiap user bagian karena setiap user sudah memiliki username dan password masing-masing disetiap bagian.
d. Sistem SIMPUS belum di lengkapi dengan Automatic Log Off.

Menurut Peraturan Menteri Kesehatan No 24 tahun 2022 tentang Rekam medis pasal 29 menjelaskan bahwa *Confidentiality* (Kerahasiaan) merupakan jaminan Keamanan data dan informasi dari gangguan pihak internal maupun eksternal yang tidak memiliki hak akses (otorisasi), sehingga data dan informasi yang ada dalam Rekam medis Elektronik terlindungi penggunaan dan penyebarannya.

Di Puskesmas Tasikmadu Karanganyar Keamanan Data SIMPUS di tinjau berdasarkan aspek *Confidentiality* dimana saat *log-in user* sudah mempunyai *username* dan *password* di setiap bagiannya masing- masing. Pada saat otentikasi (pengaksesan pengguna yang sah) SIMPUS di Puskesmas Tasikmadu Karanganyar bisa di lakukan oleh *user* pemberi pelayanan saja yang mempunyai hak otentikasi (hak akses), jadi tidak semua orang bisa mengakses aplikasi SIMPUS menggunakan hak akses tidak sah (otorisasi), untuk sistem *log-out* langsung *log-out* saja, tidak ada penerapan dalam pembuatan *password* nya. Hal itu sudah sesuai dengan SOP/III/211 Tentang Sistem Informasi Manajemen Puskesmas (SIMPUS) yang menyatakan bahwa petugas *log-in* pada aplikasi SIMPUS sesuai password masing-masing. Tetapi, hasil penelitian ini belum sesuai dengan Sudra (2020) yang menyatakan bahwa untuk meminimalkan dimana pengguna tidak sah memanfaatkan sistem yang sedang aktif, maka perlu ditunjang dengan Kemampuan *Automatic Log Off.*

Kegunaan *log off* yaitu untuk mengganti penggunaan user berbeda pada satu komputer dengan menutup semua program yang sedang berjalan, dan juga melindungi aplikasi SIMPUS dari gangguan pihak yang tidak berhak dengan melakukan *Log off* sistem aplikasi SIMPUS. Di Puskesmas Tasikmadu Karanganyar belum di lengkapi dengan *Automatic Log Off* (ALO) jadi belum bisa menonaktifkan secara otomatis, apabila petugas pengguna meninggalkan pada keadaan saat *log-in* maka sistem tersebut dapat digunakan oleh orang yang tidak berkepentingan (otorisasi). Maka dari itu perlu adanya evaluasi terkait Keamanan data di *aspek confidentiality* di mana saat sistem ditinggalkan oleh petugas pengguna tidak *Automatic Log Off* sehingga sistem dapat di akses oleh pengguna yang tidak berhak (otorisasi) dan bisa berakibat pada kebocoran informasi maka dari itu perlu adanya sistem *Automatic Log Off* atau bisa dilakukan *Log off* sistem aplikasi SIMPUS pada saat meninggalkan aplikasi sesaat. Hal tersebut sudah sesuai dengan penelitian Fitriyani *et.al*., (2016) yang menyatakan bahwa sistem SIMPUS belum dilengkapi dengan *Auto log off* ketika tidak dipergunakan dalam waktu tertentu dan fitur integritas.

Keamanan Data SIMPUS di tinjau Berdasarkan Aspek *Integrity*

Berdasarkan hasil wawancara dan observasi dengan ketiga responden tersebut menyatakan bahwa tidak ada batasan saat perubahan atau pengeditan data. Dapat disimpulkan terkait hasil wawancara dan hasil observasi ditinjau dari aspek *Integrity* sebagai berikut:

a. Proses pegeditan data dapat dilakukan oleh *user* di bagiannya masing- masing dengan mengklik tombol edit.

b. Penghapusan data hanya bisa dilakukan oleh *user* yang berwenang yaitu admin SIMPUS
c. Tidak ada batasan waktu saat merubah dan mengedit data.

Menurut Nurul Hayaty 2020 tentang Sistem Keamann menjelaskan bahwa *integrity* (keaslian) berarti menjamin bahwa data/informasi yang dimiliki terjaga keasliannya, tidak berubah tanpa pemilik informasi. Di dalam *integrity* terdapat 2 mekanisme pengamanan yaitu mekanisme priventif dan mekanisme detektif. Mekanisme priventif merupakan kontrol akses untuk menghalangi terjadinya modifikasi data. Sedangkan mekanisme detektif adalah untuk melakukan deteksi terhadap modifikasi yang telah dilakukan oleh orang lain.

Di Puskesmas Tasikmadu Karanganyar Keamanan SIMPUS di tinjau berdasarkan aspek *integrity* dimana saat pengeditan data di SIMPUS bisa dilakukan di bagianya saja seperti perawat hanya bisa mengedit bagian kolom perawat, dokter hanya bisa mengedit dibagiannya saja dan saat pengeditan data tidak ada batasan waktu. Tetapi untuk penghapusan data hanya berhak dilakukan oleh pihak yang berwenang saja atau administator SIMPUS. Hal ini sudah sesuai dengan Sudra (2020) yang menyatakan bahwa intregritas mengandung informasi yang tersedia hanya di ubah atau diolah untuk kebutuhan tertentu dan oleh pengguna tertentu yang berhak.

Hal ini juga sudah sesuai dengan penelitian Sofia, *et.al*., (2022) yang menyatakan bahwa pertimbangan integritas ketika menerapkan catatan kesehatan elektronik di fasilitas kesehatan dilakukan dengan perubahan atau penghapusan data oleh administrator.

Keamanan Data SIMPUS di tinjau Berdasarkan Aspek *Availability*

Berdasarkan hasil wawancara dan observasi dapat disimpulkan terkait ditinjau dari Aspek *Availability* sebagai berikut:

a. Data selalu bisa diakses kapanpun dan dimanapun saat data dibutuhkan.
   Kendala *server down user* tetap melakukan pengentrian data ke SIMPUS tetapi dalam mode *offline* setelah *server* kembali normal maka di lakukan singkronisasi data dan setelah itu data yang sudah di entry sudah kembali ke mode *online.*
b. *Back-up* data masih dilakukan manual dilakukan secara periodik dan bisa dilakukan setiap hari, dan data *back-up* tersimpan di komputer *server, google drive* dan komputer atas admin yang masih satu gedung.

Menurut Peraturan Menteri Kesehatan No 24 tahun 2022 tentang Rekam medis pasal 29 menjelaskan bahwa ketersediaan merupakan jaminan data dan informasi yang ada dalam Rekam medis Elektronik dapat diakses dan digunakan oleh orang yang telah memiliki hak akses yang ditetapkan oleh Pimpinan Pelayanan Kesehatan.

Di Puskesmas Tasikmadu Karanganyar keamanan data SIMPUS di tinjau berdasarkan aspek *Availability* keadaan dimana saat data dibutuhkan pasti tersedia dan bisa diakses dimanapun tempatnya, hal tersebut sudah sesuai dengan Sudra (2020) yang menyatakan bahwa petugas pelayanan kesehatan akan lebih lancar menjalankan tugasnya bila informasi yang dibutuhkan selalu siap pada saat dibutuhkan.

SIMPUS di Puskesmas Tasikmadu Karanganyar untuk proses *back-up* data belum dilakukan *otomatis back-up* data 24 jam masih di lakukan *back-up* data manual yang dilakukan secara *periodic* dan juga bisa dilakukan setiap hari. Untuk *back-up* datanya dilakukan dengan cara mem*back-up* semua data ke komputer *server, google drive* dan di komputer atas yang disimpan dalam bentuk file *data base msyql* yang tidak bisa dibuka disembarang program tetapi masi dalam satu gedung. Tetapi Puskesmas Tasikmadu Karanganyar sudah mengupayakan untuk mengusulkan ke Dinas Kesehatan untuk bisa membantu menyimpan *back-up* an data di luar gedung tersebut. Hal tersebut sudah sesuai dengan SOP/III/211 tentang Sistem Informasi Manajemen Puskesmas (SIMPUS) yang menyatakan bahwa petugas melakukan *back-up* data secara berkala dan hasil *back-up* disimpan pada media yang ada (*hard disk* eksternal/komputer lain) untuk keamanan. Tetapi, hasil penelitian ini belum sesuai dengan Sudra (2020) yang menyatakan bahwa sistem juga harus memiliki kemampuan untuk penyalinan data (*back-up)* tanpa mengganggu fungsi- fungsi lainnya dan mampu membangun informasi dari salinan data tersebut. Maka dari itu perlu adanya evaluasi terkait terkait keamanan data di aspek *availability* dimana saat sistem menyimpan bisa otomatis tersimpan di *back-up* an data guna mengantisipasi peretasan data pasien. Hal tersebut sesuai dengan penelitian Sofia, *et.al*., (2022) yang menyatakan bahwa pada penerapan rekam medik elektronik di fasilitas kesehatan dibuktikan dengan dapat

terhubungnya sistem informasi kesehatan dengan perusahaan lain khususnya BPJS kesehatan, serta menggunakan proses *backup data* otomatis guna mengantisipasi peretasan data pasien. Apabila sistem mengalami gangguan buruk di Puskesmas Tasikmadu Karanganyar tetap melakukan pengentrian data ke SIMPUS tetapi dalam *mode offline*, jika *server* kembali normal maka dilakukan singkronisasi data dan data yang di *entry* dalam keadaan *offline* menjadi *online* kembali dan juga melakukan enkripsi data.

SIMPULAN

Keamanan data SIMPUS di tinjau berdasarkan aspek *confidentiality*, dimana saat *user log-in* ke aplikasi SIMPUS sudah menggunakan hak *otentikasi* seperti memliliki *username* dan *password* di setiap bagianya masing- masing sehingga tidak semua orang bisa *log-in*. Terkait kesalahan *entry* data menjadi tanggung jawab setiap *user* bagian. Hanya saja SIMPUS belum dilengkapi dengan *Automatic Log Off*.

Keamanan data SIMPUS di tinjau berdasarkan aspek *integrity* dimana dalam aspek ini sudah dikatakan aman karena data saat diakses bisa diedit oleh pengguna pelayanan dibagiannya saja dan untuk penghapusan data hanya bisa dilakukan oleh admin SIMPUS atau pihak yang berwenang.

Keamanan SIMPUS di tinjau berdasarkan aspek *availability* dimana dalam aspek ini sudah menujang keamanan data karena saat data dibutuhkan pasti tersedia, data SIMPUS juga bisa diakses dimanapun asalkan *user* memiliki otentikasi (hak akses) seperti *username* dan *password*, hanya saja untuk SIMPUS belum dilengkapi *back-up* data otomatis tersimpan dikomputer *server* yang hidup 24 jam.

SARAN

Perlu adanya evaluasi keamanan data dalam aspek *confidentiality* dimana saat sistem ditinggalkan oleh petugas tidak *Automatic Log Off*, sistem tidak dapat diakses oleh pengguna yang tidak berhak yang dapat berakibat pada kebocoran informasi, maka dari itu petugas diharapkan untuk *log-off* dari aplikasi SIMPUS ketika meninggalkan komputer meskipun sesaat.

Perlu adanya evaluasi keamanan data dalam aspek *availability* dimana pada saat data tersimpan belum menerapkan *back-up* data otomatis 24 Perlu adanya evaluasi keamanan data dalam aspek *availability* dimana pada saat data tersimpan belum menerapkan *back-up* data otomatis 24 jam, untuk itu perlu adanya *back-up* data otomatis yang langsung tersimpan di komputer *server*, komputer atas, *google drive*, dan perlu dilakukan penyimpanan data di luar gedung (Dinas Kesehatan) agar data tetap aman dan dapat dipulihkan kembali sewaktu-waktu guna mengantisipasi peretasan data pasien.

REFERENSI

Arsip Nasional Republik Indonesia. 2021. Peraturan Arsip Nasional Republik Indonesia Nomor 15 tahun 2021. *Tentang Sistem Manajemen Keamanan Informasi di Lingkungan Arsip Nasional Republik Indonesia*. Jakarta

Barsasella, D. 2012. *Sistem Informasi Kesehatan* . *Jakarta*: Mitra Wacana Medika

Fitriyani ME, Rohmadi, Mulyono S. 2016 Tinjauan Fitur Keamanan Data Pada Pilar Unit Rekam Medis Sistem Informasi Manajemen Rumah Sakit (Simrs), *Jurnal Security Features, Hospital Management Information System* : 15 (2003-2015), [diakses pada tanggal 28 Januari 2024]. Tersedia pada: https://ejurnal.stikesmhk.ac.id/index.php/rm/article/view/591

Hayaty, N. 2020 *Sistem Keamanan.* Teknik Informatika: Universitas Maritim Raja Ali Haji

Kemenkes RI. 2017. Peraturan Menteri Kesehatan RI Nomor 46 Tahun 2017. *Tentang Strategi E-Kesehatan Nasional*

_____. 2019. Peraturan Menteri Kesehatan RI Nomor 31 Tahun 2019. *Tentang Sistem Informasi Puskesmas*

_____. 2019. Peraturan Menteri Kesehatan RI Nomor 43 Tahun 2019. *Tentang Pusat Kesehatan Masyarakat*

_____. 2022. Peraturan Menteri Kesehatan RI Nomor 24 Tahun 2022. *Tentang Rekam Medis*

Pradita, Riska, Et Al. Pentingnya Aspek Keamanan Informasi Data Pasien Pada Penerapan Rme Di Puskesmas. *Journal of Sustainable Community Service, 2022, 2.2: 52-62.* [diakses pada tanggal 28 Januari 2024] Tersedia pada: https://transpublika.co.id/ojs/index.php/JSCS/article/view/437

Qamaddin, Sallu S. 2020, Keamanan Data Pembelajaran Online Jaringan Komputer Di Perguruan Tinggi. *Jurnal Instruksional, Vol 2, No 1,* Universitas Muhammadiyah Jakarta. [Diakses Pada Tanggal 22 Maret 2024] Tersedia Pada: https://jurnal.umj.ac.id/index.php/instruksional/article/download/9436/5567

Rahardjo, Budi. 2017. *Keamanan Sistem Informasi Berbasis Internet. Bandung: PT Insan Infonesia*. [diakses pada tanggal 8 Februari 2024]. Tersedia pada: https://www.kajianpustaka.com/2022/10/keamanan-informasi.html

Saputra HN, Jamroni. 2017. Analisis Keamanan Data Sistem Informasi Di Puskesmas Pleret Bantul Yogyakarta, *Jurnal Ilmiah Ilmu Keperawatan dan Ilmu Kesehatan Masyarakat* Volume. 12, No. 2, pp. 96–105, 2017. [diakses pada tanggal 2 Februari 2024]. Tersedia pada: http://journal.stikessuryaglobal.ac.id/index.php/SM/article/view/85

Sofia S, et.al,. 2022. Analisis Aspek Keamanan Informasi Pasien Pada Penerapan RME di Fasilitas Kesehatan. *Jurnal Rekam Medik dan Manajemen Informasi Kesehatan RAMMIK*. Vol. 1, No. 2, Oktober 2022, hlm. 94 – 103 EISSN: 2829-4777. [diakses pada tanggal 6 Februari 2024] Tersedia pada: https://rammik.pubmedia.id/index.php/rmik/article/view/29

Sudra, RI. 2020. *Rekam Medis Edisi ketiga*. Tanggerang Selatan: Universitas Terbuka.

Tiorentap DRA, Hosizah. 2020, Aspek Keamanan Informasi dalam Penerapan Rekam Medis Elektronik di Klinik Medical Check-Up MP, *Jurnal Prosiding 4 Senwodipa 2020 Electronic Medical Records, Information security, ISO 27001* ISBN 978-623-6566-34-3, 2020, [diakses pada tanggal 4 Februari 2024]. Tersedia pada: https://prosiding.esaunggul.ac.id/index.php/FHIR/article/view/71