IMPLEMENTING SECURITY MECHANISMS IN HOSPITAL INFORMATION SYSTEMS: A REVIEW

[1]Rumondang Christin[*], [2]Sucipto, [3]Santi Lestari, [4]Riskha Apriliya
[1,2,3,4]STIKes Widya Dharma Husada Tangerang, Jl. Pajajaran No.1, Banten 15417, Indonesia
E-mail: christinerumondang@gmail.com

ABSTRAK

Rekam medis mengandung nilai kerahasiaan yang harus dijaga dengan baik karena isi rekam medis mengandung riwayat pengobatan pasien dari awal sampai akhir pasien tersebut berobat. Oleh sebab itu, rumah sakit berkewajiban menjaga keamanan rekam medis pasien. Sistem Informasi Manajemen dalam pengelolaan rumah sakit harus memiliki aspek keamanan dalam prosesnya. Aspek penting yang mempengaruhi keamanan pada sistem informasi manajemen sendiri salah satunya ialah *Authentication* dan *Privacy*. Tujuan penelitian ini untuk mengetahui fitur keamanan pada sistem informasi manajemen rumah sakit (SIMRS) pada unit rekam medis. Jenis penelitian ini adalah penelitian deskriptif kualitatif dengan teknik pengumpulan data yaitu wawancara dan observasi. Subjek penelitian ini adalah kepala rekam medis, kepala IT dan petugas rekam medis. Sedangkan objek dalam penelitian ini adalah sistem infomasi manajemen rumah sakit (SIMRS) di unit rekam medis. Berdasarkan hasil penelitian, yaitu sudah memiliki SPO keamanan SIMRS terutama di unit rekam medis. Keamanan SIMRS dalam hal *Authentication* belum semua petugas rekam medis memiliki *username* dan *password*nya masing-masing serta pengguna tidak pernah mengganti *password* sesuai dengan ketentuan. Keamanan SIMRS dalam hal *Pivacy* belum adanya fitur *logout* otomatis yang berguna untuk menjaga SIMRS menjadi lebih *privacy.* Dari penelitian ini adalah sebaiknya diharapkan untuk Rumah Sakit XYZ setiap petugasnya memiliki *username* dan *password*nya masing-masing serta diberikan fitur untuk *logout* secara otomatis.

Kata Kunci: (Keamanan, Sistem Informasi Manajemen Rumah Sakit)

ABSTRACT

Medical records contain confidentiality values that must be maintained properly because the contents of the medical record contain the patient's medical history from the beginning to the end of the patient's treatment. Therefore, the hospital is obliged to maintain and maintain the safety of patient medical records. Management Information Systems in hospital management must have security aspects in the process. One of the important aspects that affect the security of the management information system itself is Authentication and Privacy. Purpose of this research is to find out the security features of the hospital management information system in the medical record unit. This type of research is a qualitative descriptive research with data collection techniques, namely interviews and observation. The subjects of this study were the head of medical records, head of IT and medical record officers. While the object of this research is the hospital management information system in the medical record unit. Based on the results of the study, namely already having a SIMRS security SPO, especially in the medical record unit. SIMRS security in terms of Authentication not all medical record officers have their own username and password and users never change passwords in accordance with the provisions. SIMRS security in terms of Pivacy there is no automatic logout feature that is useful for maintaining SIMRS to be more privacy. From this research, it is best hoped that for the XYZ Hospital, each officer has their own username and password and is given a feature to log out automatically.
Keyword: (Security, Hospital Management Information System)

PENDAHULUAN

Rumah Sakit adalah institusi pelayanan kesehatan yang menyelenggarakan pelayanan kesehatan perorangan secara paripurna yang menyediakan pelayanan rawat inap, rawat jalan dan gawat darurat (Permenkes RI, 2020). Setiap rumah sakit mempunyai kewajiban melakukan pencatatan dan pelaporan tentang semua kegiatan penyelenggaraan Rumah Sakit dalam bentuk Sistem informasi dan manajemen rumah sakit.

Sistem Informasi Kesehatan adalah seperangkat tatanan yang meliputi data, informasi, indikator, prosedur, teknologi, perangkat, dan sumber daya manusia yang saling berkaitan dan dikelola secara terpadu untuk mengarahkan tindakan atau keputusan yang berguna dalam mendukung pembangunan kesehatan. (Permenkes RI No. 82 Tahun 2013).

Menurut Gordon B. Davis Dan Margareth H. Olson, pengertian dari Sistem Informasi Manajemen (SIM) adalah perangkat prosedur yang terorganisasi apabila dijalankan akan memberikan umpan balik dan informasi kepada manajemen tentang masukan, proses, dan keluaran dari suatu siklus manajemen, yaitu perencanaan, pelaksanaan, evaluasi dan pengendalian.

Sistem Informasi Manajemen Rumah Sakit yang selanjutnya disingkat SIMRS adalah suatu sistem teknologi informasi komunikasi yang memproses dan mengintegrasikan seluruh alur proses pelayanan Rumah Sakit dalam bentuk jaringan koordinasi, pelaporan dan prosedur administrasi untuk memperoleh informasi secara tepat dan akurat, dan merupakan bagian dari Sistem Informasi Kesehatan (Permenkes RI No. 82 Tahun 2013).

Dalam penggunaan Sistem Informasi Manajemen Rumah Sakit dibutuhkan tenaga perekam medis. Menurut Permenkes No. 55 Tahun 2013 Tentang Penyelenggaraan pekerjaan Perekam medis pasal 1 yaitu manajemen Pelayanan Rekam medis dan informasi kesehatan adalah kegiatan menjaga, memlihara dan melayani rekam medis baik secara manual maupun elektronik sampai menyajikan informasi kesehatan di rumah sakit, praktik dokter klinik, asuransi kesehatan, fasilitas pelayanan kesehatan dan lainya yang menyelenggarakan pelayanan kesehatan dan menjaga rekaman.

SIMRS sebagai sistem informasi manajemen dalam pengelolaan rumah sakit harus memiliki akses keamanan dalam prosesnya, dikarenakan data-data pasien harus dilindungi dari gangguan pihak internal maupun eksternal. Dengan kata lain, keamanan data merupakan perlindungan terhadap data yang bersifat privat. Faktor keamanan merupakan salah satu ruang lingkup dalam penyelenggaraan SIMRS yang sangat penting terkait dengan regulasi tentang kerahasiahan data pasien rumah sakit, serta mencegah terjadinya kehilangan data yang dapat berakibat pada gangguan pelayanan dan perawatan pasien.

Keamanan (*safety*) adalah perlindungan privasi seseorang dan kerahasiaan rekam medis, keamanan juga termasuk proteksi informasi pelayanan kesehatan dari rusak, hilang atau pengubah isi data oleh pihak yang tidak berhak Hatta (2017). Rekam medis bersifat rahasia. Artinya tidak semua orang boleh membaca dan mengetahuinya. Dalam pasal 10 ayat (1) Permenkes RI 3 Nomor 269/Menkes/Per/III/2008 tentang rekam medis mengatakan bahwa informasi tentang identitas, diagnosis riwayat penyakit, riwayat pemeriksaan dan riwayat pengobatan pasien harus di jaga kerahasiaannya oleh dokter, dokter gigi, tenaga kesehatan, petugas pengelola, dan pimpinan sarana pelayanan kesehatan.

Rekam medis mengandung nilai kerahasiaan yang harus dijaga dengan baik karena isi rekam medis mengandung riwayat pengobatan pasien dari awal sampai akhir pasien tersebut berobat. Oleh sebab itu, rumah sakit berkewajiban memelihara dan menjaga keamanan rekam medis pasien. Sistem Informasi Manajemen dalam pengelolaan rumah sakit haruslah memiliki asas keamanan dalam prosesnya, dikarenakan data-data pasien harus dilindungi dari gangguan pihak internal ataupun eksternal.

Aspek penting yang mempengaruhi keamanan pada sistem informasi manajemen sendiri salah satunya ialah *Authentication* dan *Privacy*. Berdasarkan Peraturan Menteri Kesehatan RI No. 269 tahun 2008 Bab V Pasal 14 menyebutkan bahwa pimpinan sarana pelayanan kesehatan bertanggung jawab atas hilang, rusak, pemalsuan dan penggunaan oleh orang/badan yang tidak berhak terhadap rekam medis (Data Pasien). Oleh karena itu, keamanan harus sesuai dengan perkembangan yang ada.

Studi pendahuluan yang dilakukan di Rumah Sakit XYZ memiliki Sistem Informasi Manajemen Rumah Sakit di unit rekam medis dalam segi keamanan data belum berjalan dengan baik, karena masih ada petugas rekam medis yang belum memiliki *username* dan *password*nya sendiri, dimana pada *Authentication* yaitu cara untuk menyatakan keabsahan dari seorang pengguna dengan dilakukan pengisian *username* dan *password* pada saat *login.* Penggunaan *username* dan *password* yang diberlakukan kepada setiap petugas juga tidak ditentukan masa berlakunya sehingga pengguna masih menggunakan password awal yang dibuatkan oleh administrator SIMRS.

Dalam hal *Privacy* pengguna harus menunjukan bukti bahwa memang dia pengguna yang sah, sehingga pihak yang tidak berkepentingan terhadap kemanan sistem komputer dapat diketahui sedini mungkin. Keamanan SIMRS di unit rekam medis sudah diterapkannya batasan untuk seluruh user mengoperasikan seluruh modul atau menu yang ada pada SIMRS di unit rekam medis, tetapi belum adanya fitur *logout* otomatis yang membuat SIMRS menjadi lebih *privacy*. Oleh karena itu, maka peneliti tertarik untuk mengangkat judul penelitian yaitu "Implementing Security Mechanisms In Hospital Information Systems: A Review"

METODE PENELITIAN

Metode penelitian yang digunakan adalah penelitian deskriptif kualititif. Dalam penelitian ini sampel yang akan di wawancara adalah satu Kepala Rekam Medis, dua Petugas Rekam Medis dan satu Kepala IT. Teknik pengumpulan data yang digunakan peneliti yaitu pedoman wawancara dan observasi.

HASIL PENELITIAN

1. Standar Prosedur Operasional (SPO) Keamanan SIMRS di Unit Rekam Medis

SPO keamanan berhubungan dengan pedoman keamanan dalam menjalankan sistem yang ada di Rumah Sakit. Berdasarkan hasil dari wawancara bahwa di Rumah Sakit XYZ sudah memiliki SPO keamanan SIMRS terutama di unit rekam medis, tetapi belum sepenuhnya berjalan sesuai dengan SPO yang berlaku, seperti penggunaan

username dan *password* masing-masing petugas, juga dalam pergantian *password* yang harus dilakukan oleh pengguna setiap dua bulan sekali belum diterapkan. Sosialisasi yang dilakukan oleh kepala IT yaitu dilakukannya rapat online melalui zoom meeting yang dilakukan kepada kepala unit atau penanggungjawab ruangan ketika ada perubahan SPO. Adapun kendala yang terjadi, yaitu berkaitan dengan pengguna user tersebut karena tidak mengganti *password* sesuai dengan SPO yaitu dua bulan sekali.

Menurut Kusumaningrum (2019) standar prosedur operasional adalah petunjuk bagi pegawai untuk melaksanakan pekerjaan dengan standar yang telah ditetapkan. SPO adalah suatu panduan yang dikemukakan secara jelas tentang apa yang diharapkan dan diisyaratkan dari semua karyawan dalam menjalankan kegiatan sehari-hari.

Dalam hal SPO terkait keamanan di Rumah Sakit XYZ sudah memiliki SPO terkait keamanan SIMRS di unit rekam medis, tetapi belum sepenuhnya berjalan sesuai dengan SPO yang berlaku, seperti penggunaan *username* dan *password* masing - masing petugas, juga dalam pergantian *password* yang harus dilakukan oleh pengguna setiap dua bulan sekali belum diterapkan. Dalam hal SPO yang terkait yaitu, untuk *login* ke sistem komputer menginput data, memproses data serta mencetak laporan – laporan yang diperlukan, tetapi dalam kepatuhan penggunaan masih ada yang belum berjalan dengan SPO yang sudah ditetapkan.

2. Keamanan SIMRS dalam hal *Authentication* di Unit Rekam Medis

Fitur Keamanan Data *authentication* berkaitan dengan cara untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud. Berdasarkan hasil wawancara dan observasi pengamatan di Rumah Sakit XYZ pada petugas rekam medis dalam menggunakan hal pengenalan atau otentifikasi keabsahan pemilik akun untuk *login* kedalam Sistem Informasi Manajemen Rumah Sakit (SIMRS) di unit rekam medis belum semua petugas memiliki *username* dan *password*nya masing-masing. Penggunaan *username* dan *password* masih ada petugas yang belum memilikinya, dikarenakan belum diberikan *username* dan *password* oleh pihak IT.

Pembuatan *username* dan *password* yang diberikan oleh IT kebijakannya bisa diganti oleh pengguna *username* itu sendiri setelah user mendapatkan *username* dan *password* nya masing-masing. *Username* dan *password* tidak bisa diakses oleh petugas lainnya yang tidak bersangkutan atau tidak diberi izin untuk memakai *username* dan *password* petugas lainnya, tetapi jika ingin menggunakan *username* dan *password* kepala rekam medis biasanya dengan persetujuan dari kepala rekam medis itu sendiri dan setiap bulan akan selalu dimonitoring oleh pihak IT, sehingga dapat terlihat siapa saja yang menggunakan SIMRS tersebut. Kebijakan dalam mengganti *username* dan *password* telah diberlakukan, tetapi belum dilakukan oleh user dikarenakan takutnya ada kendala yang tidak diinginkan.

Authentication adalah salah satu jalan dimana otorisasi juga dapat berjalan dengan baik, apabila sistem telah membenarkan user tersebut sebagai user yang sah atau benar maka sistem akan membagi tugas untuk seorang user menggunakan SIMRS di unit

rekam medis, hal tersebut telah mendukung keamanan sistem berjalan dengan baik.

Berdasarkan hasil observasi dan hasil wawancara di Rumah Sakit XYZ setiap PPA wajib mempunyai *username* dan *password*, tetapi masih ada petugas yang belum memiliki *username* dan *password* sendiri-sendiri, dimana petugas tersebut masih menggunakan *username* dan *password* kepala rekam medis jika akan membuka SIMRS di unit rekam medis tersebut. *Username* dan *password* awal ditentukan oleh administrator SIMRS dan selanjutnya password dapat diubah sendiri oleh pengguna.

Identitas terdaftar pengguna yang sah dan *password* pada sistem informasi di Rumah Sakit XYZ menerapkan *password* yang ada berformat alfanumerik dengan tidak ada minimal karakter dan maksimal karakter *password* tidak ditentukan dan penggunaan *password* dengan mengisikan abjad atau huruf secara berurutan juga diperbolehkan oleh sistem. Menurut Isa (2014) penggunaan *password* disarankan untuk panjangnya tidak melebihi delapan karakter atau kurang dari enam karakter dan kombinasi dari alfanumerik. Minimal *password* harus ditentukan juga karena akan mempersulit ketika *hacker* ingin melacak *password* yang digunakan.

Password pengguna sistem informasi ditentukan masa berlakunya, yaitu setiap dua bulan sekali, tetapi para pengguna *user* jarang mengganti password-nya dengan alasan takut lupa atau sudah terbiasa dengan penggunaan awal *password*, sehingga pengguna masih menggunakan *password* awal yang dibuatkan oleh Administrator SIMRS. Hal ini belum sesuai dengan Isa (2014) yang menyatakan bahwa setiap beberapa saat *password* harus diganti paling sedikit tiga bulan sekali dan untuk sistem yang memiliki risiko tinggi, *password* harus lebih sering diganti.

Kebijakan yang menegaskan untuk menjaga kerahasiaan *username* dan *password* sudah ada tetapi, dalam penerapannya sendiri ternyata belum diterapkan dengan baik. Dimana kebijakan yang ada seharusnya diikuti oleh seluruh pengguna. Sehingga, setiap kali pengguna akan menggunakan komputer yang sama walaupun pengguna yang menggunakan komputer yang awal harus me*logout* akunnya terlebih dahulu dan pengguna yang berikutnya *login* kembali menggunakan akunnya sendiri. Apabila diperbolehkan menggunakan akun orang lain maka orang yang memperbolehkan menggunakan akunnya tersebut harus berani bertanggung jawab apabila terjadi kesalahan maupun penyalahgunaan data.

3. **Keamanan SIMRS dalam hal *Privacy* di Unit Rekam Medis**

Fitur keamanan *Privacy* berkaitan dengan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Berdasarkan hasil wawancara dan observasi pengamatan di Rumah Sakit XYZ pada petugas rekam medis dalam mengidentifikasi user dalam pengoperasian modul/menu yang ada pada Sitem Informasi Manajemen Rumah Sakit, tidak bisa dilakukan terhadap seluruh modul/menu yang ada di SIMRS karena modul/menu yang ada pada SIMRS sudah memiliki bagiannya masing-masing disetiap unitnya.

Pada SIMRS di Rumah Sakit XYZ belum diterapkannya fitur yang memungkinkan pengguna keluar atau *logout* otomatis jika mereka tidak melakukan aktivitas apapun

selama durasi waktu tertentu yang berarti fitur *logout* masih dilakukan secara manual dengan cara *logout* sendiri.

Kegiatan yang ada pada SIMRS juga termasuk kedalam privacy karena menyangkut keamanan dalam penggunaan SIMRS yang bisa dilihat oleh administrator SIMRS, tetapi dalam pemakaian *username* dan *password* tidak bisa dibaca oleh administrator, agar SIMRS dapat terkontrol penggunaannya.

Fitur keamanan *Privacy* berkaitan dengan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Berdasarkan hasil observasi dan hasil wawancara di Rumah Sakit XYZ terdapat beberapa sistem yang ada di Rumah Sakit XYZ sistem yang ada sudah saling terintegrasi dimana hak akses yang dimiliki antar sistem adalah hanya data yang diperlukan oleh sistem yang ada dibagian tersebut saja yang akan ditampilkan oleh sistem, yaitu setiap unit di bagian rumah sakit hanya diterapkan satu modul SIMRS yang diperlukannya saja, sehingga unit lain tidak dapat menggunakan modul SIMRS yang tidak dibutuhkan.

Sistem informasi yang digunakan juga telah menjamin aspek *privacy* yang dibuktikan dengan adanya fitur yang memungkinkan pengguna keluar atau *logout* otomatis jika mereka tidak melakukan aktivitas apapun selama durasi waktu tertentu. Berdasarkan hasil observasi dan hasil wawancara di Rumah Sakit XYZ terdapat beberapa sistem yang ada di RS belum adanya fitur *logout* otomatis sehingga, pengguna masih tetap berada didalam SIMRS walaupun sedang tidak digunakan oleh pengguna. Menurut Diva Rizky (2020) Aspek *privacy* dibuktikan dengan bentuk tidak aktifnya (melakukan *log-out* secara otomatis) sistem informasi dalam kurun waktu 5 (lima) menit tidak terjadi aktivitas yang dilakukan oleh user. Hal ini berfungsi sebagai bentuk pertahanan ataupun pencegahan dari bentuk penyalahgunaan *user.*

Fitur *privacy* pada Rumah Sakit XYZ juga dalam segi IT dalam kewenangan tentang apa yang dikerjakan pada SIMRS dapat dilihat oleh IT, karena pihak IT atau administrator SIMRS selalu melakukan monitoring terhadap pengguna masing-masing user tersebut, tetapi dalam penggunaan *username* dan *password* tidak bisa terlihat oleh bagian IT karena bagian IT hanya dapat melihat *username*nya saja

KESIMPULAN

Diketahui Standar Prosedur Operasional terkait dengan Keamanan Sistem Informasi Manajemen Rumah Sakit (SIMRS) di unit rekam medis di Rumah Sakit XYX sudah memiliki SPO. Dalam pelaksanaan dan penerapan SPO sudah cukup baik, tetapi dalam penerapan terkait keamanan masih ada kebijakan yang belum sepenuhnya diterapkan.

Dalam hal *Authentication* penerapan *username* dan *password* belum semua petugas memilikinya, kecuali seluruh PPA yang wajib mempunyai *username* dan *password*nya masing-masing di setiap bagian unitnya masing-masing. *Password* yang ada berformat alfanumerik dengan minimal dan maksimal *password* tidak ditentukan oleh sistem, juga dalam penerapan pergantian waktu *password* tidak dilakukan oleh pengguna user.

Fitur *privacy* di unit rekam medis hanya diterapkan satu modul SIMRS yang diperlukannya saja, sehingga unit lain tidak dapat menggunakan modul SIMRS yang tidak

dibutuhkan. Dalam sistem informasi fitur *logout* otomatis juga berpengaruh terhadap keamanan SIMRS yang belum diterapkan di unit rekam medis. Dalam hal segi IT juga pekerjaan yang dilakukan dalam SIMRS dapat terlihat oleh petugas IT, tetapi dalam penggunaan *username* dan *password* tidak dapat terlihat oleh IT karena bersifat *privacy.*

DAFTAR PUSTAKA

Fitriyani, Martina Eka. (2016). *Sistem Informasi Manajemen Rumah Sakit (SIMRS) Di RSUD Kabupaten Sukoharjo Tahun 2016*. Karanganyar.

Hartatik, Indah Puji. (2014). *Buku Pintar Membuat SOP (Standard Operating Procedure)*. Yogyakarta: Flashbooks.

Hatta, Gemala (2017). *Pedoman Manajemen Informasi Kesehatan Di Sarana Pelayanan Kesehatan*. Jakarta: Universitas Indonesia Prees,2013.

Ika, Listyorini Puguh. (2021). *Sistem Keamanan SIMRS di Rumah Sakit*. Surakarta. ISBN: 978-623-97527-0-5.

Irlaili, Lerisa Desti, dan Rohmadi. (2017). *Tinjauan Keamanan Sistem Informasi Manajemen Rumah Sakit berdasarkan aspek privacy, integrity, authentication di RSUD dr. Soediran Mangun Sumarso Wonogiri*. Jurnal Rekam Medis, Vol. 11. No.1.

Isa I. (2014). *Manajemen Operasional Pendukung Sistem Informasi*. Yogyakarta: Graha Ilmu.

Kusumaningrum, A. (2019). *Analisis pengaruh SIM, SOP dan jaringan Distribusi Terhadap Supply Chain Manajemen (Studi kasus pada PT. Lion Mentari Airlines).* Widya Cipta, 3(1), 1-6.

Peraturan Menteri Kesehatan Republik Indonesia Nomor 3 Tahun 2020 Tentang *Klasifikasi Dan Perizinan Rumah Sakit*. (2020).

Peraturan Menteri Kesehatan Republik Indonesia Nomor 55 Tahun 2013 Tentang *Penyelenggaraan Pekerjaan Perekam Medis*. (2013).

Peraturan Menteri Kesehatan Republik Indonesia Nomor 82 Tahun 2013 Tentang *Sistem Informasi Manajemen Rumah Sakit*. (2013).

Peraturan Menteri Kesehatan RI Nomor 24 Tahun 2022 Tentang *Rekam Medis* Jakarta: Menteri Kesehatan RI. (2022).

Peraturan Menteri Kesehatan RI Nomor 269/Menkes/Per/III/2008: Tentang Rekam Medis.

Pujihastuti, Antik, Nunik Maya Hastuti, & Novita Yuliani. (2021). *Penerapan Sistem Informasi Manajemen Rumah Sakit.* Jurnal Manajemen Informasi Kesehatan Indonesia Vol. 9 No.2, Issn: 2337-6007 (Online); 2337-585x (Printed); Doi: 10.33560/Jmiki.V9i2.377.

Puriwigati, A. N., & Buana, U. M. (2020). *Sistem Informasi Keamanan Manajemen Informasi. May.*

Purnamasari, Evita P. (2015). *Panduan Menyusun Standard Operating Procedure*. Yogyakarta: Kobis.

Rizky, Diva A.T, Hosizah. (2020). "*Aspek Keamanan Informasi dalam Penerapan Rekam Medis Elektronik di Klinik Medical Check-Up MP*," ISBN 978-623-6566-34-3

Sanoto, H. (2020). *Penyusunan Standard Operating Procedure (SOP) Pada Dinaspendidikan Kabupaten Bengkayang Dalam Rangka Peningkatan Mutu Manajemen Organisasi.* Scholaria: Jurnal Pendidikan dan Kebudayaan 10(3), 263-268.

Setyawan D. (2017). *Handout Sistem Informasi Kesehatan Rekam Medis Elektronik (RME)*. Surakarta: Politeknik Kesehatan Surakarta.

Sofia, Siti. dkk. (2022). *Analisis Aspek Keamanan Informasi Pasien Pada Penerapan RME di Fasilitas Kesehatan.* Jember: Jurnal Rekam Medik dan Manajemen Informasi Kesehatan. EISSN: 2829-4777.

Suryaden, (2021). *PP 47 tahun 2021 tentang Penyelenggaraan Bidang Perumahsakitan*. Jakarta: Jogloabang.

Undang-Undang RI Nomor 44 Tahun 2009. Tentang Rumah Sakit. (2009). Jakarta: Sekretariat Kabinet Republik Indonesia.

Waisantoro, Data Unggul. dkk. (2014). *Tinjauan Penerapan Otentifikasi Keamanan Sistem Informasi Managemen Rumah Sakit Umum Daerah Surakarta*. Surakarta. Vol.VIII. No.1