INNOVATIVE: Journal Of Social Science Research
Volume 4 Nomor 3 Tahun 2024 Page 17410-17421
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Cyber Security Dalam Sistem Informasi Rumah Sakit Indonesia: Kajian Literatur

Aurel Artamevia Edrian Eka Suci[1✉], Inge Dhamanti[2]
(1) Department of Health Policy and Administration, Faculty of Public Health, Universitas Airlangga, Surabaya, Indonesia,
(2) Center of Excellence for Patient Safety and Quality, Universitar Airlangga, Surabaya, Indonesia,
Email: aurel.artamevia.edrian-2020@fkm.unair.ac.id[1✉]

Abstrak

Sistem Informasi Manajemen Rumah Sakit berpengaruh positif terhadap pelayanan rumah sakit. Namun, masalah keamanan data kesehatan menjadi tantangan, terutama di Indonesia. Oleh karena itu, perlindungan data kesehatan melalui keamanan siber sangat penting untuk melindungi privasi pasien. Tujuan : mengidentifikasi faktor dan solusi dalam meningkatkan keamanan data pada sistem informasi rumah sakit di Indonesia. Metode : kualitatif dengan pendekatan literatur review. Penelusuran dilakukan pada database *Google Scholar* dengan tahun terbit 5 tahun terakhir. Keyword yang digunakan yakni *cyber security, cybercrime, cyber terrorism, terrorism, data, medical, hospital, information system, information security, policy, patient, Indonesia.* Dari 315 artikel yang ditemukan, 5 artikel memenuhi kriteria inklusi. Hasil : Diperoleh 4 artikel yang membahas factor penyebab keamanan data kesehatan di Indonesia rentan serta solusi yang ditawarkan. Simpulan : Hasil kajian menunjukkan faktor penyebab kerentanan keamanan sistem informasi di rumah sakit Indonesia: sumber daya manusia, regulasi, dan infrastruktur. Pengembangan sumber daya manusia terlatih penting melalui pelatihan keamanan siber; kolaborasi antara pemerintah dan komunitas keamanan siber perlu diperkuat. Regulasi yang jelas dan infrastruktur IT medis yang terintegrasi menjadi kunci menjaga keamanan data kesehatan di rumah sakit.

Kata Kunci : *Keamanan Siber, Kejahatan Siber, Terorisme Siber, Terorisme, Data, Rumah Sakit, Medis, System Informasi, Keamanan Informasi, Kebijakan, Pasien, Indonesia.*

Abstract

The development of information technology influences hospital services through the implementation of Hospital Information Management Systems. However, the issue of data security poses a challenge, especially in Indonesia. Therefore, safeguarding healthcare data through cybersecurity is crucial for protecting patient privacy. Objective: To identify factors and solutions to enhance data security in hospital information systems in Indonesia. Method: Qualitative with a literature review approach. The search was conducted on the Google Scholar database for publications from the last 5 years. Keywords used were cyber security, cybercrime, cyber terrorism, terrorism, data, medical, hospital, information system, information security, policy, patient, Indonesia. Out of 315 articles found, 5 articles met the inclusion criteria. Results: Four articles discussing the factors causing vulnerability of health data security in Indonesia and the offered solutions were obtained. Conclusion: The study results indicate the factors causing vulnerability of information system security in Indonesian hospitals: human resources, regulations, and infrastructure. Developing trained human resources through cybersecurity training is crucial; collaboration between the government and cybersecurity communities needs to be strengthened. Clear regulations and integrated medical IT infrastructure are key to maintaining health data security in hospitals.

Keyword : *Cyber Security, Cybercrime, Cyber Terrorism, Terrorism, Data, Medical, Hospital, Information System, Information Security, Policy, Patient, Indonesia*

PENDAHULUAN

Perkembangan teknologi informasi di dunia semakin pesat seiring dengan perkembangan zaman. Di era digital ini, seluruh kegiatan menggunakan teknologi canggih salah satunya adalah pelayanan di rumah sakit. Sistem Informasi Manajemen Rumah Sakit menurut Peraturan Menteri Kesehatan Republik Indonesia Nomor 82 Tahun 2013 merupakan suatu sistem komunikasi dan teknologi informasi yang mengolah serta menggabungkan semua tahapan pelayanan di Rumah Sakit dalam bentuk koordinasi jaringan, pelaporan, dan prosedur administrasi guna mendapatkan data yang tepat dan akurat. Implementasi system informasi manajemen rumah sakit sangat diperlukan untuk mengintegrasikan seluruh pelayanan yang ada di Rumah Sakit (Fadilla & Setyonugroho, 2021). Adanya system informasi dapat meminimalisir terjadinya kesalahan dalam pengelolaan data sehingga dapat meningkatkan kinerja rumah sakit (Husni & Putra, 2019).

Inovasi system informasi rumah sakit tidak hanya memberikan manfaat tetapi juga membawa masalah baru yakni kerentanan keamanan data kesehatan. Menurut data dari Indeks Keamanan Siber Global (GCI) tahun 2017, Indonesia merupakan peringkat 70 dari 195 negara dalam hal keamanan siber (Nistrina, 2019). Oleh karena itu, Indonesia sering menjadi target serangan kejahatan siber. Pada tahun 2017, terdapat insiden serangan siber di dua

rumah sakit besar Indonesia oleh Ransomware WannyCry (Sari et al., 2020). Dampaknya, tenaga kesehatan tidak dapat mengakses informasi kesehatan dan untuk memulihkannya, rumah sakit harus membayar kepada pelaku kejahatan.

Data kesehatan merupakan hak asasi manusia yang harus dilindungi. Oleh karena itu, system informasi rumah sakit membutuhkan kemanan siber untuk melindungi data pasien dari ancaman siber (D. N. Mohan et al., 2020). *Cyber Security* merupakan praktik mengamankan jaringan, perangkat, dan data terhadap akses yang tidak sah atau penggunaan illegal (Zhang et al., 2022). *Cyber security* berfungsi untuk memastikan privasi informasi, aksesibilitas, dan integritas yang dikirimkan dalam internet. Penting bagi rumah sakit memiliki keamanan siber agar data kesehatan tidak disalahgunakan oleh pihak yang tidak bertanggungjawab.

Kejahatan siber menjadi ancaman dan sangat merugikan bagi negara. Oleh karena itu, penelitian ini bertujuan untuk menggali factor yang menyebabkan rentannya keamanan data kesehatan di Indonesia. Dari faktor-faktor tersebut, dapat diperoleh alternatif solusi untuk meningkatkan keamanan data dalam system informasi rumah sakit di Indonesia.

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini yakni Penelitian Kualitatif dengan pendekatan literatur review atau tinjauan pustaka. Sumber data yang digunakan dalam penelitian ini adalah data sekunder. Data sekunder yang dimaksud berupa jurnal nasional dan internasional (*free full text*). Strategi pencarian artikel melalui internet pada database *Google Scholar* dengan tahun terbit 5 tahun terakhir yakni dari tahun 2018 hingga tahun 2023. Keyword yang digunakan yakni *cyber security, cybercrime, cyber terrorism, terrorism, data, medical, hospital, information system, information security, policy, patient, Indonesia.*

Pemilihan artikel disesuaikan dengan tujuan penulisan yakni mencari faktor yang menyebabkan rentannya data kesehatan di Indonesia. Dari faktor-faktor tersebut, dapat diperoleh alternatif solusi untuk meningkatkan keamanan data dalam system informasi rumah sakit di Indonesia. Studi yang memenuhi kriteria inklusi adalah artikel yang diterbitkan dalam jangka waktu 5 tahun terakhir yang relevan dengan tujuan penulisan dan terbatas pada negara Indonesia. Desain penelitian tidak dibatasi pada penelitian kualitatif dan kuantitatif. Hasil penelusuran diperoleh 315 artikel. Kemudian dilakukan penyaringan melalui judul dan abstrak sehingga terdapat 5 artikel yang memenuhi kriteria inklusi yakni terbit tahun 2018 hingga 2023, *free full text*, dan sesuai dengan kriteria inklusi.

HASIL DAN PEMBAHASAN

Berdasarkan hasil penelusuran, terdapat dua artikel di publikasi tahun 2018, dua artikel di publikasi tahun 2019, dan satu artikel di publikasi tahun 2020. Lokasi penelitian dari kelima artikel dapat dilihat pada Tabel 1. Dari lima artikel terpilih, 2 artikel menggunakan metode penelitian kuantitatif (n=1) dan (n=2). Sedangkan 3 artikel menggunakan metode penelitian kualitatif dengan pendekatan empiris (n=3) dan wawancara dan pengumpulan data (n=5), serta 1 artikel menggunakan metode penelitian penelusuran kepustakaan dan dokumen kebijakan (n=4). Seluruh artikel diterbitkan pada Google Scholar. Rangkuman dari hasil penelitian dapat dilihat pada Tabel 1.

Berdasarkan tinjauan yang dilakukan menunjukkan bahwa terdapat beberapa factor yang menyebabkan kerentanan keamanan data kesehatan di Indonesia. Berdasarkan Tabel 1, masalah yang banyak ditemukan adalah sumber daya manusia yang kurang kompeten dan belum adanya regulasi terkait keamanan data kesehatan di Indonesia. Penelitian yang dilakukan oleh (Diwan et al., 2018) menunjukkan bahwa infrastruktur yang ada untuk system informasi rumah sakit kurang memadai. Dari tinjauan yang telah dilakukan dapat disimpulkan bahwa terdapat 3 faktor yang menyebabkan data kesehatan di Indonesia sering menjadi target serangan siber. Faktor tersebut antara lain sumber daya manusia, regulasi atau peraturan, dan infrastruktur.

Tabel 1. Literature Review *Cyber Security* dalam Sistem Informasi Rumah Sakit Indonesia

Nama Penulis (Tahun)	Tujuan Penelitian	Metode Penelitian	Sampel / Populasi Penelitian	Lokasi Penelitian	Hasil
Chandrika et al., 2018	Tujuan penelitian ini yakni membahas terkait ancaman *cyber* di Indonesia dan memberikan solusi kepada pemerintah untuk	Metode penelitian yang digunakan yakni kuantitatif dengan penyebaran kuesioner secara online selama 5 hari.	128 responden	Indonesia	Faktor : Faktor yang menyebabkan *cyber security* rentan yakni kurangnya pemahaman dan kesadaran rakyat Indonesia terkait kejahatan siber. Solusi : Pemerintah memberikan edukasi tentang cyber terrorism untuk membantu masyarakat menemukan solusi melawan ancaman tersebut. Diharapkan pemerintah dapat bekerjasama dengan negara maju yang memiliki keamanan tinggi. Selain itu, membentuk aliansi sistem keamanan

Nama Penulis (Tahun)	Tujuan Penelitian	Metode Penelitian	Sampel / Populasi Penelitian	Lokasi Penelitian	Hasil
	mengatasinya.				data dengan memanfaatkan sumber daya manusia yang ahli di bidangnya.
Nistrina, 2019	Untuk mengetahui tingkat keamanan informasi di *Hospital Information System*.	Penelitian yang digunakan adalah metode kuantitatif dengan kuesioner yang mengacu pada kerangka kerja COBIT 5 untuk mengevaluasi tingkat keamanan system informasi manajemen rumah sakit .	Penelitian ini menggunakan teknik *purposive sampling* dengan melibatkan 86 responden staf rumah sakit yang menggunakan system informasi manajemen rumah sakit.	Rumah sakit Soreang, Bandung, Indonesia.	Faktor : Cyber security rentan karena penggunaan perangkat lunak dan komputer ilegal serta aktivitas tidak sah. Kesadaran masyarakat Indonesia terhadap cyber security sangat rendah, sehingga masih banyak terjadi penyalahgunaan dan kehilangan data, termasuk data rumah sakit. Solusi : evaluasi keamanan informasi pada SIMRS menggunakan kerangka kerja COBIT 5 untuk mengidentifikasi area yang perlu ditingkatkan. Penelitian ini merekomendasikan peningkatan prosedur standar operasional perangkat keras dan identifikasi staf yang terlibat dalam manajemen keamanan informasi. Selain itu, pengelolaan sumber daya manusia dan respons organisasi terhadap tekanan regulatif juga penting dalam manajemen keamanan informasi di rumah sakit.
Sari et al., 2020	Untuk mengidentifikasi permasalahan terkait keamanan dalam	Metode penelitian yang digunakan adalah metode kualitatif dengan pendekatan empiris. Pengumpulan data	5 pakar keamanan informasi dari Badan Siber dan Sandi Negara.	Indonesia	Faktor : Tiga faktor utama yang membuat cyber security rentan adalah konflik nilai regulator, integritas dan keamanan data, serta privasi dan kerahasiaan data. Masalah utamanya adalah belum adanya regulasi khusus terkait keamanan

Nama Penulis (Tahun)	Tujuan Penelitian	Metode Penelitian	Sampel / Populasi Penelitian	Lokasi Penelitian	Hasil
	implementasi eHealth di Indonesia yang melibatkan pemangku kepentingan nya.	dilakukan dengan diskusi kelompok focus. Proses analisis data menggunakan pengkodean tematik yang selanjutnya dimasukkan ke dalam alat analisis ATLAS. ti 8.			informasi di layanan kesehatan. Keterbatasan sumber daya dan bias terhadap nilai privasi juga memperburuk situasi. Solusi : Membuat kebijakan eHealth di Indonesia dengan mempertimbangkan kepentingan semua pemangku kepentingan sehingga diharapkan dapat mengurangi konflik dalam penerapannya.
Sutandra, 2019	Penelitian ini bertujuan untuk menganalisis system keamanan data pasien di Indonesia dalam tinjauan kebijakan.	Metode penelitian yang digunakan adalah penelusuran kepustakaan dan dokumen kebijakan yang berkaitan dengan system keamanan data digital.	Tidak ditemukan dalam artikel.	Indonesia	Faktor : Faktor yang menyebabkan kemanan siber rentan yakni belum ada peraturan secara spesifik yang mengatur system keamanan data pasien berbasis digital. Solusi : Melakukan sosialisasi undang-undang ITE agar masyarakat memahami hak dan kewajibannya dalam era digital di Indonesia. Pemerintah juga perlu mengeluarkan regulasi khusus untuk mendukung digitalisasi di sektor kesehatan..
Diwan et al., 2018	Penelitian ini bertujuan untuk mengusulkan keamanan informasi kerangka manajemen	Metode yang digunakan adalah kualitatif melalui kegiatan wawancara, pengumpulan data, analisis, evaluasi, dan rekomendasi. Penelitian dilakukan	Tidak disebutkan dalam artikel	Rumah sakit universitas	Faktor : Infrastruktur IT medis di rumah sakit rentan karena koneksi jaringan tidak stabil, pengelolaan sistem informasi yang buruk akibat staf kurang kompeten, dan kekurangan tenaga kerja. Solusi : melakukan manajemen risiko dan laporan mitigasi risiko untuk

Nama Penulis (Tahun)	Tujuan Penelitian	Metode Penelitian	Sampel / Populasi Penelitian	Lokasi Penelitian	Hasil
	risiko untuk rumah sakit.	dengan melakukan observasi terhadap infrastruktur IT di rumah sakit universitas.			memecahkan masalah keamanan informasi yang ada di rumah sakit.

PEMBAHASAN

Sumber Daya Manusia

Sumber daya manusia memiliki peran penting dalam mengelola dan menjaga keamanan system informasi di rumah sakit. Pengembangan sumber daya manusia yang berkualitas dan kompeten sangat penting untuk menjaga keamanan data (Permana, 2021). Hal ini diperkuat dengan penelitian yang dilakukan oleh Mastaneh & Mouseli (2023) yang mengungkapkan bahwa sumber daya manusia yang kompeten dan terlatih sangat penting dalam penggunaan system informasi kesehatan secara efektif dan efisien. Penelitian yang dilakukan oleh Sari et al (2021) juga mengungkapkan bahwa sumber daya manusia berperan penting sebagai factor yang mempengaruhi kesadaran keamanan system informasi di fasilitas layanan kesehatan.

Dari hasil tinjauan diperoleh masalah yakni kurangnya wawasan dan kesadaran sumber daya manusia terkait keamanan siber. Solusi yang dapat diberikan untuk mengatasi masalah tersebut yakni dengan *capacity building*. *Capacity building* merupakan proses pembelajaran secara berkala dalam rangka mengembangakan kapasitas (Suprapto et al., 2021). Pelatihan dan edukasi merupakan salah satu upaya yang dapat dilakukan untuk meningkatkan wawasan dan kesadaran sumber daya manusia dalam mengelola system informasi rumah sakit sehingga dapat terjamin keamanannya. Pelatihan dan edukasi berisi tentang penjelasan terkait ancaman keamanan siber yang dapat terjadi, cara pengelolaan system informasi rumah sakit, dan langkah pencegahan yang dapat dilakukan untuk meminimalisir risiko serangan siber. Dengan meningkatkan pemahaman dan kesadaran sumber daya manusia akan keamanan siber, diharapkan kemanan data dalam system informasi di rumah sakit dapat terjaga.

Menurut penelitian yang dilakukan oleh Lindi Chandrika et al (2018), pemerintah perlu melakukan kerjasama atau kolaborasi untuk memperkuat keamanan data dalam system informasi di rumah sakit. Sumber daya manusia menjadi kunci utama dalam pembentukan

asosiasi dalam melawan ancaman cyber terorisme. Keberhasilan dalam melawan ancaman siber bergantung pada ketersediaan dan kualitas sumber daya manusia. Kolaborasi dapat dilakukan dengan membentuk komunitas keamanan siber untuk melawan kejahatan siber Budi et al (2021). Komunitas tersebut dapat berasal dari sumber daya manusia di Indonesia yang memiliki kemampuan lebih di bidang informatika. Selanjutnya, komunitas tersebut bekerjasama dengan lembaga pemerintah seperti Kominfo, Unit Kejahatan Siber Polri, dan Kementerian Kesehatan untuk memperkuat keamanan system informasi di rumah sakit.

Regulasi atau Peraturan

Peraturan merupakan hal dasar yang harus dimiliki oleh negara untuk memperkuat keamanan system informasi rumah sakit. Hal ini diperkuat dengan penelitian yang dilakukan oleh (Özdemir Sönmez et al., 2022) yang menyebutkan bahwa penting untuk menyusun peraturan terkait keamanan data. Hal ini bertujuan untuk melindungi data dan privasi individu dari akses yang tidak sah atau illegal. Penelitian serupa yang dilakukan oleh (Argaw et al., 2020) menyebutkan bahwa regulasi berperan penting dalam mengatur dan mengawasi penggunaan system informasi di rumah sakit. Selain itu, regulasi dapat menjamin data medis terjaga kerahasiannya.

Dari hasil tinjauan artikel disebutkan bahwa belum ada regulasi spesifik untuk melindungi data kesehatan di Indonesia. Peraturan yang ada hanya mengatur secara umum terkait system keamanan data berbasis digital. Hal tersebut tertuang dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Tidak adanya regulasi yang spesifik menyebabkan kesulitan dalam penerapan keamanan system informasi rumah sakit. Ketidakjelasan regulasi menimbulkan beberapa masalah yakni memiliki risiko tinggi terhadap penyalahgunaan data kesehatan yang berkaitan dengan privasi data seperti penyalahgunaan data pasien dan data internal rumah sakit.

Regulasi yang jelas penting untuk menjaga keamanan system informasi rumah sakit. Dengan adanya regulasi data kesehatan tidak dengan mudah disalahgunakan atau diakses oleh pihak yang tidak berwenang. Maka dari itu, penting bagi pemerintah untuk menetapkan regulasi atau peraturan terkait keamanan system informasi dalam bidang kesehatan. Hal tersebut bertujuan untuk melindungi keamanan data kesehatan dan memastikan bahwa pihak yang terlibat dalam ekosistem kesehatan mematuhi standar keamanan yang telah ditetapkan. Dengan adanya regulasi yang kuat, pemilik data dapat merasa lebih terlindungi dan percaya bahwa data mereka akan dijaga dengan baik dan tidak disalahgunakan. Oleh karena itu, regulasi yang spesifik sangat penting dalam menjaga keamanan data.

Infrastruktur

Infrastruktur memiliki peran penting dalam membangun keamanan system informasi di rumah sakit. Hal ini diperkuat dengan penelitian yang dilakukan oleh Stirano et al (2021) yang menyebutkan bahwa infrastruktur berperan penting dalam melindungi keamanan data di sektor kesehatan. Hal ini dikarenakan infrastruktur menjadi target utama serangan siber sehingga perlu dilindungi dengan memberikan solusi keamanan yang tepat. Penelitian serupa dilakukan oleh Maskun et al (2021) yang menyebutkan bahwa infrastruktur yang handal dan aman harus menjadi prioritas dalam implementasi system informasi di rumah sakit.

Menurut penelitian yang dilakukan oleh Diwan et al (2018) menunjukkan bahwa infrastruktur IT medis yang ada di rumah sakit memiliki kerentanan. Kerentanan tersebut bersalah dari kurangnya perlindungan data dan keberadaan pihak ketiga yang mengelola data kesehatan tanpa jaminan bahwa data akan dijaga kerahasiaannya. Infrastruktur dan regulasi merupakan dua hal yang saling berkaitan. Oleh karena itu, infrastruktur yang terintegrasi dengan baik dan diatur dengan regulasi yang jelas dan efektif sangat penting dalam menjaga keamanan data kesehatan.

Infrastruktur memiliki peran penting dalam membangun pertahanan keamanan system informasi di rumah sakit. Infrastruktur yang dibutuhkan untuk membangun pertahanan siber meliputi fasilitas dan infrastruktur bangunan/lokasi pusat data, NOC, laboratorium, dan fasilitas pendukung lainnya seperti pusat pemulihan data, jaringan data, aplikasi administrasi pertahanan siber, aplikasi teknis khusus untuk pertahanan siber, dan teknologi eksklusif (perangkat keras dan perangkat lunak yang mendukung aktivitas pertahanan siber tertentu). Oleh karena itu, infrastruktur yang memadai sangat penting untuk membangun pertahanan siber yang kuat dan andal.

SIMPULAN

Hasil kajian literature review menunjukkan bahwa faktor yang menyebabkan kerentanan keamanan sistem informasi di rumah sakit Indonesia dapat dikelompokkan dalam tiga kategori: sumber daya manusia, regulasi, dan infrastruktur. Pengembangan sumber daya manusia yang berkualitas dan terlatih sangat penting untuk menjaga keamanan sistem informasi di rumah sakit. Solusi yang disarankan adalah capacity building melalui pelatihan dan edukasi tentang ancaman keamanan siber, pengelolaan sistem informasi rumah sakit, dan langkah-langkah pencegahan. Kolaborasi antara pemerintah dan komunitas keamanan siber juga diperlukan untuk memperkuat keamanan data dalam sistem informasi di rumah sakit.

Regulasi sangat penting dalam memperkuat keamanan sistem informasi rumah sakit. Namun, saat ini Indonesia belum memiliki regulasi khusus untuk melindungi data kesehatan. Pemerintah perlu menetapkan regulasi yang jelas dan efektif dalam bidang keamanan sistem informasi kesehatan untuk memastikan perlindungan data yang lebih baik.

Kerentanan infrastruktur IT medis juga menjadi masalah yang perlu diatasi, terutama terkait perlindungan data dan pengelolaan data oleh pihak ketiga. Oleh karena itu, infrastruktur yang terintegrasi dengan baik dan diatur oleh regulasi yang jelas sangat penting dalam menjaga keamanan data kesehatan. Infrastruktur yang memadai, termasuk fasilitas bangunan, lokasi pusat data, jaringan data, serta aplikasi dan teknologi pendukung pertahanan siber, menjadi kunci untuk membangun pertahanan siber yang kuat dan andal.

DAFTAR PUSTAKA

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*(1), 146. https://doi.org/10.1186/s12911-020-01161-7

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO)*, *3*, 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

D. N. Mohan, S. Sagar Gowda, & I. S. Vikyath. (2020). Cyber Security in Health Care. *International Journal of Research in Engineering, Science and Management*, *3*(1).

Diwan, S. A., Computer Science and Information Technology College, University of Wasit, Wasit, Iraq, Ghaleb, M. H., Computer Science and Information Technology College, University of Wasit, Wasit, Iraq, Abd, M. H., & Computer Science and Information Technology College, University of Wasit, Wasit, Iraq. (2018). Risk Management Framework and Evaluation:Detail Site Study and Governance of InformationSecurity Risk Management in Medical InformationTechnology Infrastructure in Hospitals. *Indian Journal of Science and Technology*, *11*(14), 1–14. https://doi.org/10.17485/ijst/2018/v11i14/121300

Fadilla, N. M., & Setyonugroho, W. (2021). *Sistem Informasi Manajemen Rumah Sakit Dalam Meningkatkan Efisiensi: Mini Literature Review*. *8*(1).

Husni, M., & Putra, D. M. (2019). *ANALISIS IMPLEMEMNTASI SISTEM INFORMASI MANAJEMEN RUMAH SAKIT (SIMRS) PADA UNIT KERJA REKAM MEDIS DI RSU ' AISYIYAH PADANG*. *2*(1).

Lindi Chandrika, K., Perdana Adiperkasa, R., & Ningtyas, Y. (2018). Cyber terrorism in Indonesia. *Bulletin of Social Informatics Theory and Application*, *2*(2), 65–72. https://doi.org/10.31763/businta.v2i2.115

Maskun, Rian Nugraha, & Hasbi Assidiq, Muhammad Tayyib, Armelia Syafira. (2021). Harmonization Over the Regulations of Electronic Medical Records and its Potential to be Abused. *Medico-Legal Update*, *12*(1). https://doi.org/10.37506/mlu.v21i1.2592

Mastaneh, Z., & Mouseli, A. (2023). Holistic View on Information Systems as Logistic in Health Sector. *Evidence Based Health Policy, Management and Economics*. https://doi.org/10.18502/jebhpme.v7i1.12356

Nistrina, K. (2019). *Information Security For Hospital Information System Using Cobit 5 Framework*.

Özdemir Sönmez, F., Hankin, C., & Malacaria, P. (2022). Decision support for healthcare cyber security. *Computers & Security*, *122*, 102865. https://doi.org/10.1016/j.cose.2022.102865

Permana, A. (2021). Indonesia's Cyber Defense Strategy in Mitigating The Risk of Cyber Warfare Threats. *Syntax Idea*, *3*(1), 1. https://doi.org/10.36418/syntax-idea.v3i1.860

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

Sari, P. K., Handayani, P. W., & Hidayanto, A. N. (2020). Security Value Issues on eHealth Implementation in Indonesia. *IOP Conference Series: Materials Science and Engineering*, *879*(1), 012040. https://doi.org/10.1088/1757-899X/879/1/012040

Sari, P. K., Prasetio, A., Candiwan, Handayani, P. W., Hidayanto, A. N., Syauqina, S., Astuti, E. F., & Tallei, F. P. (2021). Information security cultural differences among health care facilities in Indonesia. *Heliyon*, *7*(6), e07248. https://doi.org/10.1016/j.heliyon.2021.e07248

Stirano, F., Lubrano, F., Vitali, G., Bertone, F., Varavallo, G., & Petrucci, P. (2021). Cross-Domain Security Asset Management for Healthcare. In H. Abie, S. Ranise, L. Verderame, E. Cambiaso, R. Ugarelli, G. Giunta, I. Praça, & F. Battisti (Eds.), *Cyber-Physical Security for Critical Infrastructures Protection* (Vol. 12618, pp. 139–154). Springer International Publishing. https://doi.org/10.1007/978-3-030-69781-5_10

Suprapto, S., Rifdan, R., & Gani, H. A. (2021). Nurse capacity building strategy in health services in hospitals. *Linguistics and Culture Review*, *5*(S1), 832–838. https://doi.org/10.21744/lingcure.v5nS1.1467

Sutandra, L. (2019). Pengaruh Sistem Pengamanan Data Pasien di Rumah Sakit Menuju Era Revolusi Industri 4.0. *Journal of Health Science and Physiotherapy*, *1*(2), 106–114. https://doi.org/10.35893/jhsp.v1i2.20

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Zhang, Z., Hamadi, H. A., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. *IEEE Access*, *10*, 93104–93139. https://doi.org/10.1109/ACCESS.2022.3204051