JOURNAL SYNTAX IDEA
p–ISSN: 2723-4339 e-ISSN: 2548-1398
Vol. 6, No. 07, Juli 2024

PERILAKU KESADARAN KEAMANAN SISTEM INFORMASI PADA SUMBER DAYA MANUSIA KESEHATAN DI LAYANAN KESEHATAN – NARRATIVE LITERRATURE REVIEW

Elsa Adila Ramadhian, Adang Bachtiar, Puput Oktamianti, Cicilya Candi
Universitas Indonesia, Indonesia
Email: cicilyacandi@ui.ac.id, adang@post.harvard.edu, oktamianti@gmail.com

Abstrak

Dalam era digital saat ini, menjaga kerahasiaan dan keamanan sistem informasi merupakan sebuah tantangan tersendiri. Industri terutama kesehatan saat ini melakukan investasi besar dalam teknologi informasi. Masih banyak kasus yang terjadi di lapangan, terutama terkait perilaku kesadaran pengguna informasi kesehatan. Tenaga medis menjadi salah satu faktor besar dalam insiden keamanan yang terjadi di layanan kesehatan. Saat ini belum banyak yang membahas mengenai faktor-faktor individu yang mempengaruhi perilaku kesadaran keamanan sistem informasi terutama di layanan kesehatan. Oleh karena itu, tujuan penulis melakukan penelitian ini adalah untuk memberikan tinjauan mengenai perilaku kesadaran kemanan sistem informasi pada sumber daya manusia (SDM) kesehatan di layanan kesehatan, mengumpulkan metode dan faktor penentu yang dapat meningkatkan perilaku kesadaran. Metode penelitian dengan kuantitatif yang disajikan dalam bentuk Narrative Litterature Review, diambil dari jurnal ilmiah untuk ditinjau. Hasil penelitian menunjukan pengaruh dari pelatihan yang telah diberikan kepada tenaga medis, lama pengalaman kerja serta aturan dan hukuman berlaku yang ada di layanan kesehatan terhadap perilaku keamanan sistem informasi pada SDM kesehatan di layanan kesehatan.

Kata Kunci: sistem informasi kesehatan, perilaku keamanan, sumber daya manusia kesehatan, tenaga medis, tenaga kesehatan, layanan kesehatan

Abstract

In today's digital era, maintaining the confidentiality and security of information systems is a challenge in itself. The industry, especially healthcare, is currently making large investments in information technology. There are still many cases that occur in the field, especially related to the behavior of health information users. Medical personnel are one of the major factors in security incidents that occur in health services. Currently, there is not much discussion about individual factors that affect information system security awareness behavior, especially in health services. Therefore, the purpose of this study is to provide a review of information system security awareness behavior in health human resources (HR) in health services, collect methods and determinants that can improve awareness behavior. The quantitative research method presented in the form of a Narrative Litterature Review, was taken from scientific journals for review. The results of the study show the influence of the training that has been given to medical personnel, the length of work experience and the

How to cite:	Elsa Adila Ramadhian, Adang Bachtiar, Puput Oktamianti, Cicilya Candi (2024) Perilaku Kesadaran Keamanan Sistem Informasi Pada Sumber Daya Manusia Kesehatan di Layanan Kesehatan – Narrative Literrature Review, *(06) 07,*
E-ISSN:	2684-883X
Published by:	Ridwan Institute

applicable rules and penalties in health services on the security behavior of information systems in health human resources in health services.

***Keywords**: Health Information Systems, Security Behaviors, Health Human Resources, Medical Personnel, Health Workers, Health Services*

PENDAHULUAN

Penggunaan sistem informasi berbasis elektronik merupakan hal yang makin dikembangkan saat ini. Mulai dari bidang akademis, industrial hingga kesehatan sudah menggunakan sistem atau pun aplikasi digital. Hal ini tentunya meningkatkan penggunaan internet sehingga risiko kebocoran data akan semakin tinggi (Maurseth, 2018). Pelaku kebocoran data pada umumnya menggunakan perangkat lunak berbahaya dan mensabotase komputer pengguna, telepon genggam ataupun jaringan komunikasi. Walaupun alat perlindungan umumnya telah dipasang pada alat komunikasi, penelitian menyebutkan hal tersebut tidak sepenuhnya memitigasi pelanggaran keamanan data (Zwilling et al., 2022).

Sistem informasi dalam bidang kesehatan merupakan bagian infrastruktur layanan kesehatan modern. Penggunaan teknologi sistem informasi dan komunikasi memberikan manfaat besar dalam efisiensi operasional, ketepatan diagnosa, dan pengelolaan data pasien. Secara global, industri layanan kesehatan di dunia sedang mengalami ancaman serangan sistem informasi. Banyak perangkat medis yang memiliki kerentanan keamanan terhadap hal tersebut, di mana rekam medik yang dikembangkan secara digital menjadi salah satu sasaran peretas. Pelanggaran keamanan data bidang kesehatan ini tentunya dapat merugikan secara reputasi, finansial, serta nyawa pasien (Sari et al., 2021) Informasi dapat disimpan dengan mudah dan pemiliknya pun bisa diubah, serta dapat terjadi referensi silang sehingga kemugkinan informasi pribadi dapat terungkap tanpa persetujuan penggunanya (Öğütçü et al., 2016).

Di Indonesia telah berlaku peraturan Menteri Kesehatan yang mengatur pengelolaan rekam medis elektronik serta Undang-undang perlindungan data pribadi. Tenaga kesehatan memiliki akses besar terhadap data pasien, sehingga kesadaran terhadap kemananan informasi merupakan aspek krusial. Melihat kasus yang terjadi beberapa tahun lalu, terjadi kebocoran data dan informasi kesehatan penduduk Indonesia. Banyak dari pasien dirugikan dengan dengan bocornya data NIK, nomor telepon serta alamat yang dapat digunakan untuk kejahata (Khalifatullah et al., 2022). Di Internasional, pada tahun 2019 terjadi peretasan *database* Ilmu Kesehatan Otoritas di Singapura, sehingga 808.000 pengguna terdampak (Hathaliya & Tanwar, 2020).

Pada dunia kesehatan di Indonesia saat, tentunya rekam medik menjadi hal utama yang dalam sistem informasi Kesehatan, terutama setelah adanya Permenkes no. 24 tahun 2022 yang mengatur mengenai rekam medik elektronik. Di dalam buku "Distrupsi Digital dan Masa Depan Rekam Medis, 2022", terdapat beberapa syarat rekam medis elektronik di Indonesia yang harus dipatuhi, yaitu *Privacy dan Confidentiality*. Rekam medis elektronik harus menjaga kerahasiaa pasien secara adekuat, untuk pencegahan akses yang tidak semestinya. Kedua yaitu *Integrity dan Integrasi.* Dimana data disimpan secara benar, tidak dimanipulasi dan selaras dengan standar yang sudah ditetapkan. Ketiga yaitu *Authentication,* mengharuskan adanya proses identifikasi dan verifikasi pengguna yang mengakses rekam medis elektronik yang tujuannya adalah memastikan hanya orang yang berwenang yang memiliki akses dan mengelola data rekam medis elektronik. Selanjutnya yang keempat yaitu *availability,* dalam rekam medis elektronik mengacu kepada tersedianya sistem

berkesinabungan sehingga para pengguna dapat mengakses informasi pasien saat dibutuhkan. Kelima yaitu *Access Control*, mengacu pada pengaturan siapa yang berhak untuk akses, mengubah, menghapus data dalam rekam medis elektronik (Sylvia Anjani & Maulana Tomy Abiyasa, 2023).

Kesadaran keamanan informasi terutama di bidang kesehatan sama dengan keamanan informasi pada umumnya yang diartikan sebagai usaha untuk menjaga keamanan informasi yang meliputi perlindungan *privacy*, *integrity* dan *availability* 8. Hal ini sudah tertuang dalam syarat rekam medis elektronik sehingga pada dasarnya wajib diterapkan. Apabila terdapat kelalaian pengelolaan rekam medik elektronik, dapat berdampak hukuman pidana dan atau denda seperti yang tertuang dalam Undang-undang nomor 27 tahun 2022 tentang Pelindungan Data Pribadi serta sanksi administratif berdasarkan Permenkes nomor 24 tahun 2022 tentang Rekam Medis.

Tujuan penulisan jurnal ini adalah membahas kesadaran keamanan sistem informasi pada SDM kesehatan di layanan kesehatan, sehingga mengetahui secara umum masalah dan faktor apa saja yang dihadapi di rumah sakit terkait kesadaran kemanan informasi pada SDM kesehatan di dalamnya.

METODE PENELITIAN

Tahap pengambilan dan pengolahan data yang dilakukan yang pertama adalah mengidentifikasi pertanyaan penelitian, dilanjutkan mencari metode untuk mengidentifikasi studi yang relevan dengan topik penelitian, melakukan seleksi studi, *charting* data, membuat kesimpulan dan pelaporan hasil yang ditemukan.

Studi bertujuan mengambil data dan informasi serta merangkum jurnal yang sudah diterbitkan sebelumnya untuk mengidentifikasi perilaku kesadaran keamanan pada tenaga terkait sistem informasi layanan kesehatan. Menceritakan kembali dalam bentuk *Narrative Literatur Review* dengan mengumpulkan, menyeleksi, mengekstraksi, dan mengkaji artikel ilmiah yang relevan dengan topik penelitian. sehingga dapat diketahui apa saja faktor saja yang berpengaruh terhadap kesadaran keamanan sistem informasi pada tenaga medis di layanan Kesehatan. Ruang lingkup penelitian ini dibatasi dengan framework PICO (*Population/Problem, Intervention, Comparison, Outcomes*).

Studi diambil di beberapa situs yang terpercaya yaitu dari Pubmed, Sage Journal, Science Direct, Nature dan Google Scholar. Kata kunci yang digunakan untuk mencari penelitian adalah “Cyber Hygine Among Health Workers” AND “Healthcare”.

Penelitian yang dicari adalah berupa original research, practice guideline dan meta-analysis.

Tabel 1. PICO, Kriteria Inklusi dan Eksklusi Penyaringan Artikel

Komponen	Keterangan	Kriteria Inklusi	Kriteria Eksklusi
Patien/problem/population	*Healthcare Workers*	Jurnal internasional yang berhubungan dengan tenaga medis di layanan kesehatan dalam rentan tahun 2017– 2024.	Jurnal internasional yang berhubungan dengan tenaga medis di layanan kesehatan tidak dalam rentan tahun 2017– 2024.
Intervention/exposure	*Cyber Hygine / Cyber Awereness*	Jurnal yang berhubungan dengan tingkat kesadaran keamanan sistem	Jurnal yang tidak berhubungan dengan tingkat kesadaran keamanan sistem

		informasi di layanan kesehatan	informasi di layanan kesehatan
Comparative	-	-	-
Outcome	*Faktor perilaku keamanan system informasi*	Faktor-faktor yang berpengaruh pada tingkat kesadaran keamanan sistem informasi pada tenaga medis di layanan kesehatan	Tidak membahas mengenai faktor-faktor yang berpengaruh pada tingkat kesadaran keamanan sistem informasi pada tenaga medis di layanan kesehatan

HASIL DAN PEMBAHASAN

Pada pencarian artikel menggunakan situs jurnal, dilakukan seleksi berdasarkan kriterian inklusi dan eksklusi, serta penghapusan duplikasi. Dilakukan penilaian dan review dengan melihat keseluruhan isi.

Tabel 2. Artikel yang digunakan

No.	Author	Title	Country	Result
1.	(Arain et al., 2019)	*Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization*	Canada	Ada hal positif yang signifikan korelasi antara persepsi staf kesehatan tentang efektivitas materi pendidikan keamanan TI dan kepuasan terhadap keamanan TI dalam organisasi.
2.	(Solic et al., 2019)	*Awareness About Information Security And Privacy Among Healthcare Employees*	Kroasia	Tenaga medis/ karyawan layanan kesehatan yang dilibatkan dalam penelitian ini menunjukkan hasil yang sebagian lebih baik daripada karyawan rata-rata pengguna internet di Kroasia dalam hal pengetahuan dan perilaku online yang berpotensi berisiko.
3.	(Kessler et al., 2020)	*Information security climate and the assessment of information security risk among healthcare employees*	Amerika	Keamanan Informasi berhubungan dengan motivasi keamanan informasi karyawan / tenaga medis dan perilaku keamanan informasi yang lebih baik.
4.	(Alhuwail et al., 2021)	*Information Security*	Kuwait	Faktor individu yang rentan terhadap insiden keamanan

		Awareness and Behaviors of Health Care Professionals at Public Health Care Facilities		sistem infomasi yang paling berpengaruh dibandingkan indikator lain yaitu usia atau jenis kelamin.
5.	(Balakrishnan et al., 2019)	*The Moderating Effect Of Working Experience On Health Information Sistem Security Policies Compliance Behaviour*	Malaysia	Persepsi kerentanan secara signifikan mempengaruhi perilaku kepatuhan pengguna terhadap kebijakan keamanan informasi kesehatan pada kelompok yang sangat berpengalaman dan lebih kuat dibandingkan pengguna yang memiliki pengalaman rendah.
6.	(Kuo et al., 2021)	*Hospital Staff's Adherence to Information Security Policy: A Quest for the Antecedents of Deterrence Variables*	Taiwan	Pelatihan, dan kesadaran keamanan dikombinasikan dengan efektivitas audit internal merupakan prediktor signifikan terhadap tingkat keparahan hukuman dan kepastian hukuman, sedangkan dukungan manajemen tidak
7.	(Sania, 2022)	*Structural Model of the Healthcare Information Security Behavior of Nurses Applying Protection Motivation Theory*	Korea	*Coping appraisal* berpengaruh signifikan terhadap niat keamanan informasi kesehatan, sedangkan niat berpengaruh signifikan terhadap perilaku keamanan informasi kesehatan.
8.	(Jalali et al., 2020)	*Why Employees (Still) Click on Phishing Links: Investigation in Hospitals*	*USA*	Terdapat hubungan signifikan antara beban kerja dengan perilaku keamanan.
9.	(Johansson et al., 2020)	*Information Technology and Medical Technology Personnel´s Perception Regarding Segmentation of Medical Devices: A Focus Group*	Sweden	Segmentasi jaringan perangkat medis, kebijakan keamanan dan peningkatan basis pengetahuan berpengaruh terhadap keamanan sistem infomasi.

		Study		
10.	(Gordon, Wright, Aiyagari, et al., 2019)	*Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions*	*USA*	Meningkatnya kampanye / edukasi berkaitan dengan penurunan kemungkinan mengklik *email phising*, menunjukan potensi manfaat terkait simulasi dan kesadaran mengenai *phising*.
11.	(Budke & Enko, 2020)	*Physician Practice Cybersecurity Threats: Ransomware*	Missouri	Terkait perilaku keamanan sistem infomasi, untuk meminimalkan ancaman penulis menyarankan untuk melatih pengguna untuk meninjau dan memverifikasi email bersumber terpercaya sebelum mengklik link atau membuka lampiran.
12.	(Hewitt et al., 2017)	*Mobile Device Security: Perspectives of Future Healthcare Workers*	*USA*	Peningkatan pengetahuan kesadaran kemanan di kalangan profesional layanan kesehatan merupakan prioritas, salah satu cara meningkatkan tingkat adopsi mekanisme keamanan seluler.
13.	(Ghafur et al., 2019)	*The challenges of cybersecurity in health care : the UK National Health Service as Case Study.*	*England*	Kerangka kerja yang jelas dan pemahaman pengguna tentang keamanan sistem infomasi dapat meningkatkan perilaku ketahanan sistem infomasi dalam layanan kesehatan.
14.	(Gordon, Wright, Glynn, et al., 2019)	*Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system*	*USA*	Dalam penelitian ini menunjukan faktor pemberian pelatihan tidak mempunyai dampak terhadap perilaku kesadaran keamanan sistem infomasi.
15.	(Gordon, Wright, Glynn, et al., 2019)	*Phishing in healthcare organisations: threats, mitigation and approaches*	*London, UK*	Terdapat 3 faktor prediktor *phising* yang signifikan yaitu tingkat Pendidikan, kesadaran yang sudah ada sebelumnya tentang *phising* dan tingkat kinerja pada tes penilaian neuropsikologis.

16.	(Schmidt et al., 2021)	*A Simple Assessment of Information Security Awareness in Hospital Staff Across Five Danish Regions*	Denmark	Terdapat korelasi antara kepuasan terhadap teknologi informasi dengan kesadaran kemanan system informasi.
17.	(Yeo & Banfield, 2022)	*Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis*	USA	Kebijakan keamanan sistem infomasi rendah karena tenaga Kesehatan tidak menyadari risiko dari keamanan sistem infomasi yang buruk. Program pelatihan dan kesadaran mengenaik kemanan sistem infomasi perlu ditingkatkan.
18.	(Argyridou et al., 2023)	*Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Health Care Organizations: Concept Study*	Eropa	Metode pembelajaran mengenai kemanan sistem infomasi meningkatkan persepsi dan perilaku keamanan di sektor layanan kesehatan pada tenaga kesehatan.
19.	(Abdelhamid, 2020)	*The Role of Health Concerns in Phishing Susceptibility: Survey Design Study.*	*USA*	Masalah kesehatan, kecendrungan mempercayai orang lain, dan kecendrungan mengambil risiko merupakan faktor risiko dalam kerentanan *phising.* Selain itu, perempuan memiliki kerentanan *phising* lebih tinggi dibandingkan laki-laki.
20.	(Yeng et al., 2021)	*Mapping the Psychosocial cultural Aspects of Healthcare Professionals' Information Security Practices*	*Norway*	Pelanggaran data yang terjadi di layanan kesehatan disebabkan oleh faktor kurangnya pengalaman para profesional layanan kesehatan/ tenaga kesehatan dalam kemanan informasi, kurangnya pengembangan praktik dalam kesadaran keamanan dan kurangnya motivasi untuk memberi insentif kepada profesional

	layanan kesehatan.

Didapatkan 20 artikel dari hasil pencarian seperti pada tabel sebelumnya dengan topik kemanan sistem infomasi yang membahas tentang kesadaran pengguna di kalangan tenaga kesehatan dan faktor yang mempengaruhinya. Di dalam artikel melaporkan penelitian mengenai serangan sistem infomasi secara umum, serta *phising* di layanan kesehatan.

Kemanan sistem informasi merupakan upaya untuk melindungi sistem komputer, jaringan dan data dari serangan penyalahgunaan data dan akses yang tanpa izin. Dalam sistem informasi kesehatan, keamanan sistem infomasi sangat penting terkait data pasien yang bernilai tinggi dan *confidential.* Keamanan sistem informasi dipengaruhi oleh berbagai hal salah satunya perilaku keamanan dari pengguna dalam hal ini tenaga kesehatan di layanan kesehatan.

Terdapat beberapa ancaman sistem infomasi yang paling sering ditemukan di dalam organisasi Kesehatan, yaitu serangan terhadap kerentanan struktur IT terkat kesalahan konfigurasi jaringan (cotohnya *: firewall*, layanan digital yang membebani dengan banyaknya permintaan (*denial of service*), bug perangkat lunak di dalam system, eskalasi hak Istimewa, penyadapan, serangan kriptografi), serangan *ransomware* dimana ditujukan terhadap organisasi kesehatan untuk mengganggu layanan dan mengambil data penting demi keuntungan dan ancaman kerentanan manusia dalam mendapat akses infrakstruktur layanan kesehatan (Yeng et al., 2021).

Dalam artikel yang ditemukan, upaya mitigasi dilakukan dan mempengaruhi perilaku staf medis di layanan Kesehatan terhadap keamanan sistem infomasi. Diantaranya staf medis yang diberikan pendidikan/ pelatihan mengenai kesadaran keamanan sistem informasi, terdapat korelasi yang positif terhadap persepsi staf mengenai persepsi dan kepuasan terhadap keamanan sistem informasi. Dengan adanya pelatihan tersebut, staf medis memiliki kemungkinan lebih besar untuk melaporkan tindakan mereka terutama apabila terjadi perilaku yang tidak aman (Arain et al., 2019). Hal serupa juga terdapat pada artikel lainnya yang didapatkan (Humaidi & Balakrishnan, 2015; Johansson et al., 2020), dimana pelatihan, kampanye, edukasi memberikan pemahaman tentang keamanan sistem infomasi berpengaruh signifikan terhadap perilaku ketahanan kemanan sistem infomasi pada tenaga medis. Terbentuknya kerangka kerja yang jelas dan pemahaman pengguna tentang kemanan sistem infomasi, serta audit internal dapat meningkatkan perilaku ketahanan sistem infomasi dalam layanan Kesehatan (Ghafur et al., 2019; Kuo et al., 2021). Walaupun demikian ada satu penelitian yang mendapati bahwa pelatihan tidak memiliki dampak terhadap keamanan sistem infomasi, namun hal ini dipengaruhi oleh lingkungan penelitian yang cukup terbatas (Gordon, Wright, Glynn, et al., 2019).

Indeks perilaku keamanan sistem informasi dari peneltian yang dilakukan kepada empat kategori profesional kesehatan, didapatkan bahwa hal tersebut berhubungan dengan motivasi keamanan informasi karyawan dan perilaku keamanan informasi yang lebih baik (Kessler et al., 2020). Sesungguhnya petugas layanan kesehatan memiliki perilaku keamanan sistem informasi serta pengetahuan secara umum mengenai sistem keamanan informasi lebih baik dari keseluruhan rata-rata pengguna internet pada umumnya. Didiskripsikan juga bahwa petugas layanan kesehatan wanita tidak lebih berisiko dibanding laki-laki, serta usia juga mempengaruhi. Petugas yang lebih tua dikatakan jauh labih berhati-hati dan lebih jarang meminjamkan data aksesnya di tempat kerja kepada rekan kerjanya serta tenaga profesional dengan pengalaman kerja yang lebih tinggi, menunjukkan lebih tinggi pula kepatuhan terhadap keamanan sistem informasi (Alhuwail et al., 2021; Solic et al., 2019).

Kelompok tenaga kesehatan dengan pengalaman tinggi, memiliki perilaku keamanan sistem informasi lebih baik dibanding kelompok dengan pengalaman rendah karena

perbedaan persepsi kerentanan secara signifikan mempengaruhi perilaku kepatuhan pengguna terhadap kebijakan keamanan informasi kesehatan pada kelompok yang sangat berpengalaman dan lebih kuat dibandingkan pengguna yang memiliki pengalaman rendah (Humaidi & Balakrishnan, 2015; Yeng et al., 2021). Selain itu, penilaian tenaga kesehatan terhadap bahaya, berpengaruh signifikan pada niat keamanan informasi, Hal ini mempengaruhi perilaku keamanan informasi (Lee & Seomun, 2021)

Ada hal menarik, dimana disebukan bahwa terdapat juga hubungan signifikan antara beban kerja dengan perilaku keamanan sistem informasi di kalangan tenaga kesehatan 27. Masalah kesehatan, kecenderungan mempercayai orang lain dan kecendrungan mengambil risiko dalam pekerjaan merupakan faktor risiko kerentanan dalam serangan *phising* di kalangan tenaga kesehatan (Abdelhamid, 2020; Johansson et al., 2020).

Selain faktor internal dari para tenaga kesehatan pengguna sistem informasi, terdapat hubungan pada segmentasi jaringan perangkat medis dan kebijakan keamanan sistem informasi pada layanan kesehatan serta kepuasan terhadap teknologi informasi yang digunakan, memiliki peran dalam keamanan sistem informasi (Johansson et al., 2020; Schmidt et al., 2021).

KESIMPULAN

Perilaku keamanan petugas kesehatan sangat penting untuk melindungi layanan kesehatan dari ancaman keamanan sistem informasi. Karenanya sangat penting tentunya bagi tenaga Kesehatan yang bekerja, tidak hanya update ilmu mengenai medis, namun juga mengenai kemanan sistem informasi serta memahami kebijakan keamamanan sistem informasi yang relevan, yang saat ini pasti digunakan dalam pelayanan. Peran aktif tenaga kesehatan sangat diharapkan guna melindungi kerahasiaam pasien, memastikan privasi data pasien serta layanan kesehatan. Dari beberapa sumber yang diambil, didapatkan beberapa faktor yang mempengaruhi perilaku kesadaran keamanan sistem informasi pada tenaga medis di kesehatan. Disebutkan bahwa yang utama adalah pelatihan serta keilmuan mengenai kemanan sistem informasi sebaiknya diberikan secara berkala kepada seluruh tenaga medis di layanan diberikan secara berkala. Khususnya kepada tenaga medis baru di layanan kesehatan sangat disarankan agar memiliki pengetahuan mengenai keamanan sistem informasi. Hal tersebut sangat membantu mengingatkan para tenaga medis untuk berperilaku sistem informasi secara aman. Pengalaman kerja juga meningkatkan kesadaran keamanan terhadap sistem informasi, sebab semakin terpapar dengan sistem informasi makan akan semakin mengetahui hal baik dan buruk apa yang dapat terjadi apabila berperilaku tidak aman.

Selain itu layanan kesehatan perlu mengembangkan sistem informasi yang baik sehingga penggunaannya pun mudah dan dapat digunakan dengan baik oleh penggunanya terutama tenaga kesehatan. Tenaga medis yang sudah berpengalaman memiliki kesadaran tentang keamanan sistem informasi kesehatan lebih tinggi. Layaknya pengalaman dalam bekerja, paparan tinggu sehingga meningkatkan sikap yang seharusnya dalam menggunakan sistem informasi. Disarankan tenaga medis berpengalaman bekerja sama, mengarahkan tenaga kesehatan yang belum memiliki pengalaman tinggi sehingga dapat membantu terciptanya kemanan sistem informasi lebih cepat dan baik. Layanan kesehatan juga sebaiknya mengembangkan sistem penilaian terhadap tenaga medis yang bertugas di layanan kesehatan

terkait keamanan penggunaan sistem informasi yang ada sehingga memberikan efek terhadap perilaku keamanan sistem informasi kesehatan.

BIBLIOGRAFI

Abdelhamid, M. (2020). The Role Of Health Concerns In Phishing Susceptibility: Survey Design Study. *Journal Of Medical Internet Research*, *22*(5), E18394.

Alhuwail, D., Al-Jafar, E., Abdulsalam, Y., & Alduaij, S. (2021). Information Security Awareness And Behaviors Of Health Care Professionals At Public Health Care Facilities. *Applied Clinical Informatics*, *12*(04), 924–932.

Arain, M. A., Tarraf, R., & Ahmad, A. (2019). Assessing Staff Awareness And Effectiveness Of Educational Training On IT Security And Privacy In A Large Healthcare Organization. *Journal Of Multidisciplinary Healthcare*, 73–81.

Argyridou, E., Nifakos, S., Laoudias, C., Panda, S., Panaousis, E., Chandramouli, K., Navarro-Llobet, D., Mora Zamorano, J., Papachristou, P., & Bonacina, S. (2023). Cyber Hygiene Methodology For Raising Cybersecurity And Data Privacy Awareness In Health Care Organizations: Concept Study. *Journal Of Medical Internet Research*, *25*, E41294.

Balakrishnan, V., Khan, S., Fernandez, T., & Arabnia, H. R. (2019). Cyberbullying Detection On Twitter Using Big Five And Dark Triad Features. *Personality And Individual Differences*, *141*, 252–257.

Budke, C. A., & Enko, P. J. (2020). Physician Practice Cybersecurity Threats: Ransomware. *Missouri Medicine*, *117*(2), 102.

Ghafur, S., Grass, E., Jennings, N. R., & Darzi, A. (2019). The Challenges Of Cybersecurity In Health Care: The UK National Health Service As A Case Study. *The Lancet Digital Health*, *1*(1), E10–E12.

Gordon, W. J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J., Kufahl, J., Mazzone, C., Noga, J., & Parkulo, M. (2019). Assessment Of Employee Susceptibility To Phishing Attacks At US Health Care Institutions. *JAMA Network Open*, *2*(3), E190393–E190393.

Gordon, W. J., Wright, A., Glynn, R. J., Kadakia, J., Mazzone, C., Leinbach, E., & Landman, A. (2019). Evaluation Of A Mandatory Phishing Training Program For High-Risk Employees At A US Healthcare System. *Journal Of The American Medical Informatics Association*, *26*(6), 547–552.

Hathaliya, J. J., & Tanwar, S. (2020). An Exhaustive Survey On Security And Privacy Issues In Healthcare 4.0. *Computer Communications*, *153*, 311–335.

Hewitt, B., Dolezel, D., & Mcleod Jr, A. (2017). Mobile Device Security: Perspectives Of Future Healthcare Workers. *Perspectives In Health Information Management*, *14*(Winter).

Humaidi, N., & Balakrishnan, V. (2015). The Moderating Effect Of Working Experience On Health Information System Security Policies Compliance Behaviour. *Malaysian Journal Of Computer Science*, *28*(2), 70–92.

Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020). Why Employees (Still) Click On Phishing Links: Investigation In Hospitals. *Journal Of Medical Internet Research*, *22*(1), E16775.

Johansson, D., Jönsson, P., Ivarsson, B., & Christiansson, M. (2020). Information Technology And Medical Technology Personnel´ S Perception Regarding Segmentation Of Medical Devices: A Focus Group Study. *Healthcare*, *8*(1), 23.

Kessler, S. R., Pindek, S., Kleinman, G., Andel, S. A., & Spector, P. E. (2020). Information Security Climate And The Assessment Of Information Security Risk Among Healthcare Employees. *Health Informatics Journal*, *26*(1), 461–473.

Khalifatullah, A. W., Apsari, A. F., Lutfiyah, A., Qoriah, E. A., Qoriah, A., Zukhri, G. S., & Ridho, M. R. R. (2022). Perlindungan Data Pribadi Pasien Terhadap Serangan Cyber Crime. *Sanskara Hukum Dan HAM*, *1*(02), 47–53.

Kuo, K.-M., Talley, P. C., & Lin, D.-Y. M. (2021). Hospital Staff's Adherence To Information Security Policy: A Quest For The Antecedents Of Deterrence Variables. *INQUIRY: The Journal*

Of Health Care Organization, Provision, And Financing, *58*, 00469580211029599.
Lee, E., & Seomun, G. (2021). Structural Model Of The Healthcare Information Security Behavior Of Nurses Applying Protection Motivation Theory. *International Journal Of Environmental Research And Public Health*, *18*(4), 2084.
Maurseth, P. B. (2018). The Effect Of The Internet On Economic Growth: Counter-Evidence From Cross-Country Panel Data. *Economics Letters*, *172*, 74–77.
Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis Of Personal Information Security Behavior And Awareness. *Computers & Security*, *56*, 83–93.
Sania, J. (2022). *Analisis Resepsi Penonton Drama Korea True Beauty Mengenai Pertukaran Peran Gender*.
Sari, P. K., Prasetio, A., 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).
Schmidt, T., Nøhr, C., & Koppel, R. (2021). A Simple Assessment Of Information Security Awareness In Hospital Staff Across Five Danish Regions. In *Public Health And Informatics* (Pp. 635–639). IOS Press.
Solic, K., Plesa, M., Velki, T., & Nenadic, K. (2019). Awareness About Information Security And Privacy Among Healthcare Employees. *Southeastern European Medical Journal: SEEMEDJ*, *3*(1), 21–28.
Sylvia Anjani, S. K. M., & Maulana Tomy Abiyasa, A. (2023). *Disrupsi Digital Dan Masa Depan Rekam Medis (Kajian Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 Tentang Rekam Medis Elektronik)*. Selat Media.
Yeng, P. K., Szekeres, A., Yang, B., & Snekkenes, E. A. (2021). Mapping The Psychosocialcultural Aspects Of Healthcare Professionals' Information Security Practices: Systematic Mapping Study. *JMIR Human Factors*, *8*(2), E17604.
Yeo, L. H., & Banfield, J. (2022). Human Factors In Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. *Perspectives In Health Information Management*, *19*(Spring).
Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge And Behavior: A Comparative Study. *Journal Of Computer Information Systems*, *62*(1), 82–97.