JDISTIRA

Vol. 6 No.1 Tahun 2026

Pelatihan Keamanan Digital SIMRS untuk Pencegahan Kebocoran Data Pasien di RS Sentra Medika Cikarang

Anom Dwi Prakoso[1]
[1]Program Studi Sarjana Administrasi Kesehatan, Fakultas Ilmu Kesehatan, Universitas Medika Suherman
e-mail: [1]anomdwiprakoso@gmail.com

Article History
Received: 21 November 2025
Revised: 27 November 2025
Accepted: 31 Januari 2026
DOI:https://doi.org/10.58794/jdt.v6i1.1843

Keyword - Data Protection, Information Security, Data Breach, Electronic Medical Records, Hospitals.

Kata Kunci − **SIMRS, Perlindungan Data, Keamanan Informasi, Kebocoran Data, Rekam Medis Elektronik, Rumah Sakit.**

Abstract *− Digital transformation through the implementation of Hospital Management Information Systems (SIMRS) enhances efficiency and quality in healthcare services; however, it also increases the risk of patient data breaches if not supported by adequate security governance. Law No. 27 of 2022 on Personal Data Protection and Ministry of Health Regulation No. 24 of 2022 on Electronic Medical Records mandate healthcare facilities to ensure the security of patient data. Preliminary identification at RS Sentra Medika Cikarang revealed several vulnerabilities, including weak password practices, the absence of multi-factor authentication, low awareness of phishing threats, and limited understanding of data security regulations. This community engagement program aimed to improve regulatory literacy and SIMRS security skills through regulatory dissemination, technical workshops, and data breach incident simulations. A total of 43 participants took part in the training using a one-group pre–post intervention design and were evaluated through pre- and post-tests. The results showed an increase in the average score from 48.49 to 88.19, representing an 81.87% improvement. The Wilcoxon signed-rank test indicated a statistically significant difference ($p < 0.001$). In addition to cognitive improvement, participants demonstrated behavioral changes, including the adoption of strong passwords, the implementation of multi-factor authentication, and improved ability to identify and respond to phishing attempts. This program proved effective in enhancing human resource competencies and fostering a stronger information security culture within the hospital.*

Abstrak **− Transformasi digital melalui penerapan Sistem Informasi Manajemen Rumah Sakit (SIMRS) meningkatkan efisiensi dan kualitas layanan kesehatan, namun juga menimbulkan risiko kebocoran data pasien apabila tidak didukung oleh tata kelola keamanan yang memadai. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis Elektronik mewajibkan fasilitas kesehatan menjamin keamanan data pasien. Identifikasi awal di RS Sentra Medika Cikarang menunjukkan adanya kerentanan, seperti penggunaan password lemah, belum diterapkannya multi-factor authentication, rendahnya kewaspadaan terhadap phishing, serta keterbatasan pemahaman regulasi keamanan**

data. Kegiatan Pengabdian kepada Masyarakat ini bertujuan meningkatkan literasi regulasi dan keterampilan keamanan SIMRS melalui sosialisasi regulasi, workshop teknis, dan simulasi insiden kebocoran data. Sebanyak 43 peserta mengikuti pelatihan dengan desain one-group pre–post intervention dan dievaluasi menggunakan pre–post-test. Hasil menunjukkan peningkatan skor rata-rata dari 48,49 menjadi 88,19 (peningkatan 81,87%). Uji Wilcoxon signed-rank menunjukkan perbedaan signifikan (p < 0,001). Selain peningkatan kognitif, peserta menunjukkan perubahan perilaku berupa penerapan password kuat, penggunaan multi-factor authentication, serta kemampuan mengenali dan merespons phishing. Program ini terbukti efektif meningkatkan kompetensi SDM dan mendorong penguatan budaya keamanan informasi di rumah sakit.

1. PENDAHULUAN

Transformasi digital dalam pelayanan kesehatan telah menjadi agenda utama pemerintah Indonesia dalam rangka meningkatkan mutu layanan, efisiensi operasional, akurasi pencatatan medis, serta percepatan alur informasi antarunit. Implementasi Sistem Informasi Manajemen Rumah Sakit (SIMRS) merupakan bagian integral dari proses digitalisasi tersebut, karena memungkinkan rumah sakit mengintegrasikan data klinis, administratif, manajerial, dan keuangan dalam satu sistem terpadu. Penelitian menunjukkan bahwa SIMRS berkontribusi signifikan terhadap peningkatan kinerja rumah sakit melalui percepatan proses pelayanan dan dukungan pengambilan keputusan [1]. Dengan demikian, digitalisasi tidak hanya menjadi pilihan, tetapi merupakan kebutuhan strategis bagi fasilitas pelayanan kesehatan.

Meskipun memberikan berbagai manfaat, digitalisasi di sektor kesehatan menghadirkan tantangan yang kompleks, terutama terkait keamanan data dan privasi informasi pasien. Data kesehatan termasuk kategori data pribadi yang bersifat sensitif dan wajib dilindungi oleh institusi pengelola. Kebocoran data kesehatan dapat berdampak luas, baik dari aspek hukum, sosial, maupun reputasi rumah sakit. Berbagai laporan menunjukkan meningkatnya tren kebocoran data kesehatan secara global maupun nasional, di mana sebagian besar insiden terjadi akibat lemahnya proteksi sistem dan rendahnya literasi keamanan informasi SDM [2] [3]. Kondisi ini menunjukkan bahwa keamanan digital bukan hanya persoalan teknologi, tetapi juga kesiapan sumber daya manusia.

Data kesehatan merupakan data pribadi yang bersifat sensitif dan wajib dilindungi secara ketat. Kebocoran data kesehatan dapat menimbulkan dampak serius, baik dari aspek hukum, sosial, maupun reputasi institusi pelayanan kesehatan. Berbagai laporan menunjukkan meningkatnya insiden kebocoran data kesehatan secara global dan nasional, yang sebagian besar disebabkan oleh lemahnya proteksi sistem serta rendahnya kesadaran dan literasi keamanan informasi sumber daya manusia [4][5]. Hal ini menegaskan bahwa keamanan digital bukan semata persoalan teknis, melainkan juga persoalan kesiapan organisasi dan perilaku manusia.

Untuk menjawab tantangan tersebut, pemerintah telah menerbitkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP). Regulasi ini mengatur perlindungan data pribadi dalam seluruh sektor, termasuk kesehatan, serta mengamanatkan adanya mekanisme persetujuan, pengelolaan, dan pengamanan data oleh pengendali data. Selain itu, Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis Elektronik mengatur secara khusus bagaimana fasilitas pelayanan kesehatan harus mengelola rekam medis digital mulai dari penyimpanan, akses, integritas, hingga kewajiban menjaga kerahasiaan pasien. Kedua regulasi tersebut menegaskan bahwa fasilitas pelayanan kesehatan bertanggung jawab penuh atas keamanan dan keselamatan data pasien.

Namun, realitas di lapangan menunjukkan bahwa kepatuhan fasilitas kesehatan terhadap regulasi keamanan data belum optimal. Banyak rumah sakit yang masih menghadapi kendala seperti penggunaan password yang lemah, belum diterapkannya autentikasi berlapis, terbatasnya audit trail sistem, kurangnya kemampuan staf dalam mengenali potensi serangan siber, serta tidak adanya SOP respons insiden kebocoran data. Di sisi lain, minimnya pelatihan dan literasi keamanan digital di lingkungan fasilitas kesehatan sering menjadi penyebab utama lemahnya pengamanan sistem informasi [6] [1]. Hal ini menunjukkan adanya kesenjangan antara kebijakan dan implementasi di tingkat operasional.

RS Sentra Medika Cikarang, sebagai rumah sakit rujukan kawasan industri dengan volume layanan tinggi dan kompleksitas operasional yang besar, menghadapi berbagai kerentanan terkait keamanan digital. Observasi awal menemukan penggunaan *password* generik, belum diterapkannya *multi-factor authentication*, rendahnya kewaspadaan terhadap serangan phishing, serta ketiadaan prosedur baku penanganan insiden kebocoran data. Selain itu, sebagian besar tenaga kesehatan belum memahami secara komprehensif regulasi PDP maupun prinsip dasar keamanan informasi seperti konsep CIA yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Kondisi ini menunjukkan adanya *gap* serius antara tuntutan regulasi dan kapasitas keamanan informasi di lingkungan rumah sakit.

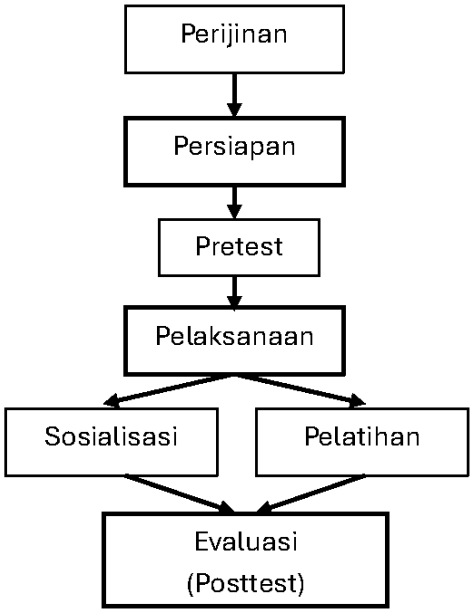
Berbagai studi menunjukkan bahwa strategi penguatan kapasitas melalui pendekatan *workshop*, simulasi insiden, dan pelatihan interaktif efektif meningkatkan kesadaran dan kemampuan tenaga kesehatan dalam menjaga keamanan data digital [7] [8]. Pendekatan edukatif dan partisipatif diperlukan peserta untuk memahami konteks risiko keamanan, mengenali ancaman, serta mempraktikkan langkah pencegahan. Selain itu, pelatihan semacam ini berperan membangun budaya keamanan informasi sebuah aspek penting yang seringkali terlupakan dalam pengembangan sistem teknologi kesehatan.

Diperlukan intervensi yang tidak hanya memberikan pemahaman regulatif, tetapi juga membekali tenaga kesehatan dengan keterampilan teknis terkait keamanan digital. Pelatihan yang mengintegrasikan sosialisasi regulasi, *workshop* praktik, dan simulasi insiden terbukti efektif dalam meningkatkan literasi keamanan serta membangun budaya keamanan informasi yang berkelanjutan [8]. Oleh karena itu, pelaksana PkM menyelenggarakan kegiatan sosialisasi regulasi PDP dan pelatihan keamanan SIMRS bagi tenaga kesehatan RS Sentra Medika Cikarang.

Tujuan kegiatan PKM ini adalah meningkatkan kapasitas SDM rumah sakit dalam memahami regulasi perlindungan data, mengimplementasikan praktik keamanan SIMRS, serta membangun budaya kerja yang berorientasi pada perlindungan data digital. Kegiatan ini diharapkan memberikan kontribusi nyata dalam memperkuat tata kelola keamanan data kesehatan dan mendukung upaya rumah sakit agar lebih siap menghadapi tantangan digitalisasi layanan kesehatan.

2. METODE PENGABDIAN (11 point)

Kegiatan Pengabdian kepada Masyarakat ini dilaksanakan di RS Sentra Medika Cikarang, Kabupaten Bekasi, pada periode September–November 2025. Program difokuskan pada peningkatan literasi regulasi dan keterampilan praktis keamanan digital dalam penggunaan SIMRS. Metode pelaksanaan menggunakan *one-group pre–post intervention design*, yang dipilih untuk mengevaluasi perubahan pengetahuan dan keterampilan peserta sebelum dan sesudah intervensi pelatihan. Desain ini dinilai sesuai karena kegiatan bersifat edukatif, melibatkan satu kelompok peserta yang sama, serta bertujuan menilai efektivitas langsung dari program pelatihan.



Gambar 1. Alur Pelaksanaan Kegiatan Pengabdian Masyarakat

Berdasarkan Gambar 1, alur kegiatan pengabdian terdiri atas tiga tahap utama dengan enam tahapan operasional. Sebelum dilaksanakan kegiatan PkM, pelaksana pengabdian terlebih dahulu **(1)melakukan koordinasi dan izin** dengan pihak manajemen rumah sakit untuk memperoleh izin pelaksanaan kegiatan sekaligus melakukan pengumpulan data dan informasi pendukung, penentuan materi sosialisasi, serta penyiapan skenario simulasi yang akan digunakan. Setelah mendapatkan perijinan, pelaksana memulai **(2)tahap persiapan**, pelaksana memastikan seluruh kebutuhan teknis seperti perangkat elektronik, jaringan internet, ruang pelatihan, serta daftar peserta sudah

siap digunakan pada hari pelaksanaan. Pelaksana juga merancang materi berbasis regulasi, terutama Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan Permenkes Nomor 24 Tahun 2022 tentang Rekam Medis Elektronik, serta menyusun instrumen *pre–post-test* yang berisi 20 soal pilihan ganda mengenai prinsip dasar keamanan informasi, *password policy*, *multi-factor authentication*, pengenalan *phishing*, dan prosedur respons insiden.

Sebelum sesi pelatihan dimulai, **(3)seluruh peserta diwajibkan mengisi *pre-test*** yang disediakan sebagai instrumen awal untuk mengukur tingkat pemahaman peserta terkait regulasi dan keamanan data sebelum menerima materi. Pada sesi awal, peserta diberikan pemahaman dasar mengenai regulasi Undang-Undang Perlindungan Data Pribadi, Permenkes 24/2022 tentang Rekam Medis Elektronik, konsep CIA, serta berbagai risiko kebocoran data yang sering terjadi di fasilitas pelayanan kesehatan.

(4)Tahap pelaksanaan kegiatan dilaksanakan tanggal 15 November 2025, kegiatan meliputi **(5)penyampaian sosialisasi, pelatihan teknis** dan *ice breaking*. Setelah sesi pemaparan materi, kegiatan dilanjutkan dengan pelatihan teknis melalui workshop. Dalam sesi ini peserta mempraktikkan cara membuat *password* kuat, menerapkan *multi-factor authentication*, mengenali serangan *phishing* dan prosedur respons insiden., Selama sesi berlangsung, peserta juga diberikan kesempatan untuk bertanya dan berdiskusi terkait pengalaman mereka menggunakan SIMRS dalam kegiatan pelayanan sehari-hari.

(6)Tahap akhir yaitu forum simulasi dan evaluasi, Evaluasi kuantitatif dilakukan dengan membandingkan skor *pre-test* dan *post-test* menggunakan uji *Wilcoxon signed-rank*, karena data bersifat berpasangan dan tidak berdistribusi normal. Evaluasi kualitatif dilakukan melalui observasi selama simulasi, diskusi kelompok, serta umpan balik peserta untuk menilai perubahan perilaku, kesiapan, dan pemahaman dalam menerapkan praktik keamanan digital. Seluruh rangkaian kegiatan didokumentasikan dalam bentuk foto, daftar hadir, dan catatan evaluasi sebagai bahan laporan dan analisis lebih lanjut.

Pelaksanaan metode pengabdian yang terstruktur dan berfokus pada praktik langsung, diharapkan mampu meningkatkan pemahaman peserta terkait regulasi serta memperkuat kesiapan tenaga kesehatan dalam mengamankan data pasien di lingkungan rumah sakit.

3. HASIL DAN PEMBAHASAN

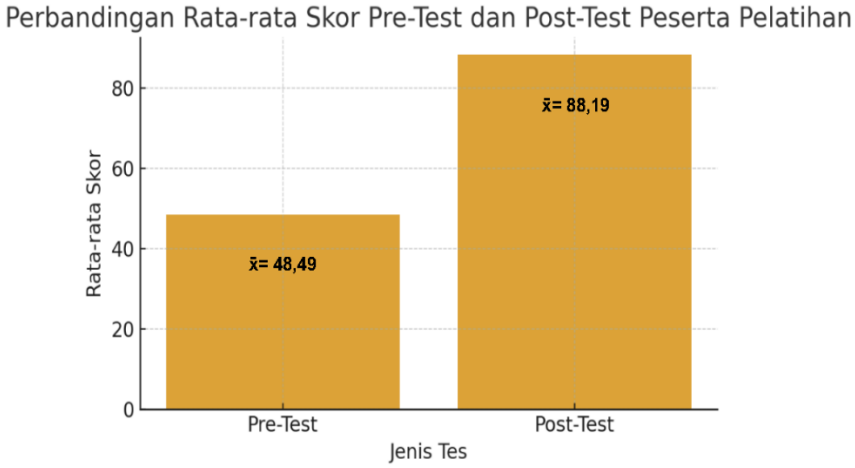
Pelaksanaan kegiatan pengabdian kepada masyarakat berupa sosialisasi regulasi perlindungan data dan pelatihan keamanan SIMRS di RS Sentra Medika Cikarang telah menghasilkan luaran yang sesuai dengan tujuan awal, yaitu meningkatkan pengetahuan dan keterampilan peserta dalam mengelola keamanan data kesehatan. Kegiatan ini berhasil menyelesaikan permasalahan mitra yang sebelumnya memiliki keterbatasan dalam pemahaman regulasi perlindungan data pribadi dan belum menerapkan standar keamanan dalam penggunaan SIMRS.

Sebelum kegiatan dilaksanakan, kondisi mitra menunjukkan beberapa permasalahan yang cukup signifikan. Berdasarkan hasi *pre-test* dan observasi pada peserta, sebagian besar pegawai RS belum memahami secara mendalam tentang prinsip keamanan data. Penggunaan *password* sederhana, kurangnya kewaspadaan terhadap ancaman *phishing*, serta belum adanya prosedur respons insiden merupakan masalah yang sering ditemui di unit kerja. Selain itu, prosedur keamanan digital belum terdokumentasi dengan baik, sehingga risiko paparan data pasien cukup tinggi.

Tabel 1. Analisis Deskriptif Nilai Pre-Test dan Post-Test Peserta Pelatihan

Statistik	Pre-Test	Post-Test
Jumlah Peserta (N)	43	43
Mean	48,49	88,19
Standar Deviasi	5,34	4,06
Nilai Minimum	39	80
Nilai Maksimum	58	96
Median	49	88

Berdasarkan Tabel 1, nilai rata-rata peserta meningkat sebesar 39,70 poin atau 81,87% setelah pelatihan. Penurunan standar deviasi pada *post-test* menunjukkan bahwa pemahaman peserta tidak hanya meningkat, tetapi juga menjadi lebih merata. Hal ini mengindikasikan bahwa metode sosialisasi regulasi dan pelatihan teknis terbukti efektif meningkatkan pemahaman seluruh peserta PkM.



Gambar 2. Grafik hasil pre-test dan post-test

Gambar 2 memperkuat temuan ini dengan menampilkan perbedaan distribusi nilai *pre-test* dan *post-test* secara visual. Grafik menunjukkan pergeseran nilai peserta dari kategori rendah–sedang ke kategori tinggi setelah intervensi, menegaskan dampak positif program pelatihan terhadap kompetensi peserta.

Tabel 2. Hasil Uji Wilcoxon

Variabel yang Diuji	**N**	**W (Wilcoxon)**	**p-value**	**Keterangan**
Skor *protes* vs *post-test*	43	0.000	$2{,}27 \times 10^{-13}$	Signifikan ($p < 0{,}05$)

Hasil uji beda menggunakan *wilcoxon signed-rank test* menghasilkan nilai W = 0,000 dan p-value = $2{,}27 \times 10^{-13}$ ($p < 0{,}05$). Hasil ini menunjukkan terdapat perbedaan yang signifikan antara nilai *pre-test* dan *post-test* peserta. Dengan demikian, kegiatan pelatihan memberikan dampak nyata terhadap peningkatan pengetahuan peserta. Pemilihan uji Wilcoxon sudah sesuai karena data selisih *pre–post* tidak berdistribusi normal dan seluruh peserta mengalami peningkatan nilai, sehingga uji parametrik seperti *paired t-test* tidak dapat digunakan.

Selain peningkatan pengetahuan, perubahan perilaku peserta juga terlihat selama proses pelatihan dan simulasi. Peserta menunjukkan peningkatan kemampuan dalam membuat password kompleks, menerapkan multi-factor authentication, serta lebih berhati-hati terhadap pesan atau tautan yang berpotensi mengandung phishing. Hasil ini sejalan dengan penelitian Nayla, Ramadhan and Riatma, (2025) dan Elendu *et al.*, (2024) yang menyatakan bahwa pelatihan interaktif berbasis simulasi mampu meningkatkan awareness dan kesiapan tenaga kesehatan terhadap ancaman keamanan digital [9] [10].

Pada sesi simulasi insiden, sebagian besar peserta mampu merespons percobaan akses ilegal dan skenario kebocoran data dengan lebih cepat dan tepat, menunjukkan peningkatan kemampuan dalam mendeteksi dan menangani ancaman keamanan. Temuan ini memperlihatkan bahwa pelatihan tidak hanya berdampak pada penguatan kompetensi kognitif, tetapi juga membangun pola perilaku dan budaya kerja yang lebih peduli terhadap keamanan data pasien. Studi Willie, (2025) dan Bonesso *et al.*, (2020) turut mendukung bahwa perubahan perilaku merupakan indikator utama keberhasilan program edukasi keamanan informasi [11] [12].

Gambar 3. Penyampaian Sosialisasi Regulasi dan Pelatihan Teknis Perlindungan Data pada SIMRS

Peserta menunjukkan antusiasme tinggi saat sesi diskusi. Diskusi dilakukan setelah simulasi juga memberikan masukan penting terkait tantangan implementasi keamanan SIMRS di lapangan. Peserta mengungkapkan bahwa kendala utama yang selama ini dihadapi adalah kurangnya pedoman operasional standar, beban kerja yang tinggi, serta minimnya pelatihan berkala yang membahas keamanan digital. Diskusi ini menunjukkan bahwa peningkatan kompetensi individu perlu diikuti dengan penguatan kebijakan internal, seperti penyusunan SOP keamanan data, audit keamanan digital, dan pembentukan mekanisme pelaporan insiden yang lebih terstruktur. Dengan demikian, hasil pelatihan tidak hanya meningkatkan pengetahuan peserta, tetapi juga memberikan rekomendasi nyata bagi manajemen rumah sakit untuk.

Meskipun pelatihan menunjukkan hasil yang positif, diskusi kelompok mengungkapkan sejumlah kendala dan hambatan implementasi di lapangan. Beberapa peserta menyampaikan adanya resistensi awal dari sebagian staf terhadap perubahan kebiasaan, terutama terkait penggunaan autentikasi berlapis yang dianggap menambah beban kerja. Selain itu, keterbatasan logistik seperti perangkat pendukung, konektivitas jaringan, serta belum tersedianya SOP keamanan data yang baku menjadi tantangan tersendiri [13] [14].

Tantangan lainnya adalah keberlanjutan praktik keamanan digital setelah pelatihan. Tanpa dukungan kebijakan institusional, seperti pelatihan berkala, audit keamanan, dan mekanisme pelaporan insiden yang jelas, perubahan perilaku individu berpotensi tidak bertahan dalam jangka panjang. Oleh karena itu, hasil temuan ini menegaskan bahwa penguatan kompetensi SDM perlu diiringi dengan komitmen manajerial dan sistem pendukung yang memadai [4][5].

Secara keseluruhan, pelaksanaan kegiatan ini menunjukkan bahwa intervensi berupa sosialisasi regulasi dan pelatihan keamanan SIMRS mampu memberikan dampak langsung terhadap kompetensi dan perilaku tenaga kesehatan di RS Sentra Medika Cikarang. Kondisi mitra setelah kegiatan menunjukkan peningkatan signifikan dari sisi pengetahuan, keterampilan, dan kesadaran akan pentingnya keamanan data. Hasil ini menjadi dasar yang kuat bagi rumah sakit untuk melanjutkan penyusunan SOP keamanan data serta memperkuat budaya keamanan informasi di masa mendatang..

4. SIMPULAN

Kegiatan pelatihan keamanan digital SIMRS di RS Sentra Medika Cikarang terbukti efektif meningkatkan pengetahuan dan perilaku peserta. Peningkatan skor *pre–post-test* yang signifikan serta perubahan praktik kerja menunjukkan keberhasilan program dalam memperkuat kompetensi SDM dan budaya keamanan informasi. Hasil kegiatan dapat menjadi dasar bagi manajemen rumah sakit dalam memperkuat tata kelola keamanan data, khususnya pada unit SIMRS dan pelayanan klinis.

5. SARAN

Rumah sakit perlu menyusun SOP keamanan data, memperkuat mekanisme pelaporan insiden, dan melakukan pelatihan serta audit keamanan secara berkala agar budaya perlindungan data dapat diterapkan secara konsisten.

UCAPAN TERIMA KASIH

Pelaksana PkM berterima kasih kepada Universitas Medika Suherman yang telah memfasilitasi pendanaan dan perizinan kegiatan serta kepada RS Sentra Medika Cikarang atas dukungan, kerja sama, dan kesediaannya menjadi mitra dalam pelaksanaan kegiatan pengabdian kepada masyarakat ini. Selain itu pelaksana PkM turut menyampaikan terima kasih kepada seluruh peserta pelatihan serta pihak-pihak lain yang berkontribusi dalam menyukseskan kegiatan ini, baik dalam bentuk dukungan moral, teknis, maupun administratif.

DAFTAR PUSTAKA

[1] P. K. Sari *et al.*, "Information security cultural differences among health care facilities in Indonesia," *Heliyon*, vol. 7, no. 6, p. e07248, 2021, doi: 10.1016/j.heliyon.2021.e07248.

[2] F. M. Dias, M. L. Martens, S. F. de P. Monken, L. F. da Silva, and E. D. R. Santibanez-Gonzalez, "Risk management focusing on the best practices of data security systems for healthcare," *Int. J. Innov.*, vol. 9, no. 1, pp. 45–78, 2021, doi: 10.5585/iji.v9i1.18246.

[3] R. Murray-Watson, "Healthcare data breach statistics. HIPAA J.," HIPAA J. Accessed: Oct. 06, 2025. [Online]. Available: https://www.hipaajournal.com/healthcare-data-breach-statistics/

[4] D. Natasya Putri, S. Hajijah Purba, K. Layana, K. Lubis, J. Lapangan Golf, and D. Jangak, "Tantangan dan Solusi dalam Implementasi SIMRS di Rumah Sakit Pemerintah di Indonesia," *JRIKUF J. Ris. Ilmu Kesehat. Umum*, vol. 3, pp. 13–22, 2025. https://doi.org/10.57213/jrikuf.v3i1.480

[5] Y. Cita *et al.*, "Tantangan Implementasi SIMRS dari Perspektif Tenaga Kesehatan : Studi Kualitatif di Rumah Sakit Daerah," Vol. 4, No. 1, Pp. 121–132, 2025. https://doi.org/10.59027/al-ihtiram.v4i1.965

[6] Wartini, I. Sartika, J. Pertiwi, and Y. Triana, "Analisis Kesiapan Implementasi Rekam Medis Elektronik Ditinjau Dari Sumber Daya Manusia Dan Sarana Dan Prasarana Di Rumah Sakit Umum Daerah Dr. Darsono Kabupaten Pacitan Provinsi Jawa Timur," *J. Manaj. Inf. dan Adm. Kesehat.*, vol. 06, no. 02, p. 2023, 2023.

[7] A. Virk, S. Alasmari, D. Patel, and K. Allison, "Digital Health Policy and Cybersecurity Regulations Regarding Artificial Intelligence (AI) Implementation in Healthcare," *Cureus*, vol. 17, no. 3, pp. 1–9, 2025, doi: 10.7759/cureus.80676.

[8] World Health Organization, and International Telecommunication Union, *Digital health platform handbook: building a digital information infrastructure (infostructure) for health*. World Health Organization, 2020.

[9] A. B. Nayla, G. R. Ramadhan, and S. Riatma, "Pelatihan dan Sosialisasi Keamanan Digital untuk Meningkatkan Kesadaran Siswa Terhadap Ancaman Phishing di Era Digital," *TrendX (Jurnal Pengabdi. Masy. Inov. dan Apl. Teknol.*, vol. 1, no. 1, pp. 39–47, 2025, [Online].

[10] C. Elendu *et al.*, "The impact of simulation-based training in medical education: A review," *Med. (United States)*, vol. 103, no. 27, p. e38813, 2024, doi: 10.1097/MD.0000000000038813.

[11] M. M. Willie, "Strategies for Enhancing Training and Development in Healthcare Management," *Adv. Hum. Resour. Manag. Res.*, vol. 3, no. 1, pp. 44–59, 2025, doi: 10.60079/ahrmr.v3i1.408.

[12] S. Bonesso, F. Gerli, R. Zampieri, and R. E. Boyatzis, "Updating the Debate on Behavioral Competency Development: State of the Art and Future Challenges," *Front. Psychol.*, vol. 11, no. June, 2020, doi: 10.3389/fpsyg.2020.01267.

[13] S. H. Nugroho and K. Gunawan, "Kepuasan Kerja Karyawan di Rumah Sakit : Review Masalah dan Prospek di Era Digital," *Rekayasa*, vol. 17, no. 3, pp. 501–507, 2024, doi: 10.21107/rekayasa.v17i3.27912.

[14] A. Fittrani, A. Rohendi, B. Sukajie, and Purwadhi, "Penguatan SDM dalam Mendukung Transformasi Digital di RSUD Dr . Adjidarmo," *J. Knowl. Manag.*, vol. 18, no. 02, pp. 055–074, 2024. https://journal.uniga.ac.id/index.php/JKM/article/view/42491