

Penyimpanan Kredensial Peramban dan Kontrol Akses Berbasis *CompTIA Security+* Terhadap Keamanan Akun SIMRS

Vander Han Andriano

Institut Teknologi & Bisnis Sabda Setia, Indonesia

vanderhan.andriano@itbss.ac.id



Histori Artikel:

Diajukan: 1 Juli 2026

Disetujui: 26 September 2026

Dipublikasi: 30 September 2026

Kata Kunci:

Kebocoran data; SIMRS; *save password*; identity and access management; *CompTIA Security+*; akuntabilitas

Digital Transformation Technology (Digitech) is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

Abstrak

Insiden kebocoran data kesehatan terus meningkat, salah satunya dipicu oleh kelemahan autentikasi dan perilaku pengguna. Di Rumah Sakit Kharitas Bhakti, tenaga medis sering menggunakan fitur "save password" pada browser di perangkat bersama (shared device) untuk mempercepat login Sistem Informasi Manajemen Rumah Sakit (SIMRS). Praktik ini menghilangkan akuntabilitas dan memicu risiko akses tidak sah. Penelitian sebelumnya baru berfokus pada aspek teknis sistem secara umum, belum menyentuh perilaku spesifik penyimpanan kredensial ini. Penelitian ini bertujuan menganalisis pengaruh perilaku penggunaan fitur "save password" (X1) dan persepsi terhadap Identity and Access Management (IAM) berbasis *CompTIA Security+* (X2) terhadap risiko penyalahgunaan akun (Y) pada SIMRS. Metode yang digunakan adalah kuantitatif melalui survei kepada 85 responden tenaga medis di Rumah Sakit Kharitas Bhakti. Hasil pengujian simultan (Uji F) menunjukkan bahwa kedua variabel independen berpengaruh signifikan terhadap risiko penyalahgunaan akun dengan kontribusi sebesar 58,5% (R Square = 0,585). Secara parsial (Uji t), fitur "save password" tidak menunjukkan pengaruh signifikan karena adanya mitigasi lingkungan fisik kerja, sedangkan pemahaman IAM berbasis *CompTIA Security+* berpengaruh positif dan sangat dominan dalam meningkatkan sensitivitas staf terhadap risiko siber. Kesimpulannya, penerapan mekanisme IAM yang ketat sesuai prinsip *CompTIA Security+* (autentikasi, otorisasi, akuntabilitas) sangat krusial untuk memitigasi risiko. Implikasi praktis penelitian ini menekankan pentingnya rumah sakit berinvestasi pada tata kelola penguatan sistem otomatis dan edukasi literasi keamanan siber bagi seluruh staf dan karyawan guna menjamin integritas serta kerahasiaan data pasien.

PENDAHULUAN

Di lingkungan operasional, Sistem Informasi Manajemen Rumah Sakit (SIMRS) memegang peran vital untuk mengintegrasikan data rekam medis dan mempercepat pelayanan. Namun, efisiensi ini sering kali terganggu oleh kerentanan keamanan yang disebabkan oleh kontrol akses yang belum optimal dan faktor perilaku sumber daya manusia dalam mengelola kredensial. Salah satu praktik buruk yang sering ditemukan di lapangan, seperti pada Rumah Sakit Kharitas Bhakti, adalah kebiasaan tenaga medis menyimpan username dan password pada peramban (browser) menggunakan fitur save password. Praktik ini umumnya dilakukan pada perangkat yang digunakan secara bersama (shared device) di ruang pelayanan dengan tujuan demi mempercepat proses login akibat tingginya beban kerja.

Dampak dari perilaku tersebut sangat fatal; peramban dapat membuka akses ke SIMRS secara otomatis tanpa melalui proses autentikasi ulang. Hal ini tidak hanya membuka celah bagi pihak yang tidak berwenang untuk menyalahgunakan akun, tetapi juga melenyapkan jejak akuntabilitas pengguna di dalam sistem jika terjadi modifikasi data ilegal. Meskipun penelitian terdahulu telah banyak mengkaji aspek teknis keamanan SIMRS, sebagian besar literatur masih berfokus pada sistem secara general dan belum secara spesifik mengulas perilaku pemanfaatan fitur save password pada perangkat bersama sebagai sumber kerentanan utama. Kekosongan riset (research gap) inilah yang mendasari dilakukannya penelitian ini. Pendekatan kuantitatif secara implisit digunakan untuk menguji secara empiris sejauh mana perilaku buruk ini meningkatkan risiko keamanan, serta bagaimana penerapan IAM berbasis *CompTIA Security+* dapat bertindak sebagai solusi mitigasi. Ruang lingkup penelitian ini difokuskan untuk menjawab bagaimana pengaruh perilaku penggunaan fitur save password dan persepsi terhadap IAM berbasis *CompTIA Security+* terhadap risiko terjadinya penyalahgunaan akun pada SIMRS di Rumah Sakit Kharitas Bhakti.

STUDI LITERATUR

Sistem Informasi Manajemen Rumah Sakit (SIMRS). Sistem Informasi Manajemen Rumah Sakit (SIMRS) adalah sistem teknologi informasi terintegrasi yang dirancang untuk mengelola seluruh alur data pelayanan kesehatan secara digital, mulai dari aspek klinis hingga administrasi (Laia dkk., 2025). Menurut Igiany (2019), SIMRS adalah bagian dari sistem informasi kesehatan yang menyediakan sumber informasi secara relevan di seluruh rumah sakit untuk mendukung pengambilan keputusan yang efektif dan administrasi rumah sakit. Meskipun integrasi ini mampu mengoptimalkan efektivitas operasional, kompleksitas sistem dan tingginya kuantitas pengguna seringkali memicu tantangan besar dalam perlindungan aset data (Simanullang dkk., 2026). Mengingat data kesehatan bersifat sangat sensitif dan memuat legalitas rekam medis pasien, jaminan kerahasiaan (confidentiality) mutlak diperlukan (Abbas dkk., 2025). Kebocoran informasi di lingkungan rumah sakit umumnya bersumber dari lemahnya kontrol autentikasi dan rendahnya literasi digital staf, sehingga diperlukan manajemen identitas akses yang lebih terstruktur (Suhirman dkk., 2026).

Fitur Save Password dan Risiko Penyalahgunaan Akun. Fitur save password merupakan mekanisme pada peramban yang berfungsi menyimpan kredensial pengguna secara otomatis guna mempermudah proses login berikutnya tanpa input berulang (Fitaliqoh & Rakhmawati, 2024). Namun, implementasi fitur ini pada lingkungan komunal dengan perangkat bersama (shared device) menimbulkan celah keamanan kritis karena meniadakan proses verifikasi ulang identitas (Bahaji, 2025). Menurut Sulianta (2024), keamanan siber adalah upaya melindungi data dan sistem komputer dari ancaman luar. Ketika aspek kenyamanan (convenience) lebih diprioritaskan daripada keamanan (security), peluang terjadinya penyalahgunaan akun oleh pihak internal maupun eksternal yang tidak berwenang akan meningkat tajam (Bilkist Ramadani dkk., 2026).

Prinsip Keamanan CompTIA Security+. CompTIA Security+ merupakan standar keamanan global yang memberikan fondasi kuat dalam mengevaluasi ketahanan sistem informasi melalui pengelolaan kontrol akses terstandarisasi (Bilkist Ramadani dkk., 2026). Dalam konteks IAM, prinsip ini mengarahkan implementasi kontrol akses berbasis peran (Role-Based Access Control) dan manajemen kredensial yang ketat untuk menjamin konsistensi pengamanan data digital organisasi.

Kerangka Konseptual dan Hipotesis. Penelitian ini memetakan hubungan kausalitas di mana kemudahan akses dari fitur save password diposisikan sebagai pemicu kerentanan, sementara kontrol ketat IAM berbasis CompTIA Security+ diposisikan sebagai penekan risiko (Abbas dkk., 2025; Suhirman dkk., 2026). Variabel dalam penelitian ini meliputi (1) Variabel Independen (X1): Penggunaan fitur save password; (2) Variabel Independen (X2): Penerapan IAM berbasis prinsip CompTIA Security+; (3) Variabel Dependen (Y): Risiko terjadinya penyalahgunaan akun. Berdasarkan kerangka tersebut, diajukan tiga hipotesis penelitian: H1: Menggunakan fitur save password berpengaruh positif terhadap risiko penyalahgunaan akun pada SIMRS. H2: Menerapkan IAM berbasis prinsip CompTIA Security+ yang berpengaruh negatif terhadap risiko dalam penyalahgunaan akun pada pengguna sistem SIMRS Rumah Sakit. H3: Menerapkan IAM berbasis prinsip CompTIA Security+ mampu memitigasi pengaruh penggunaan save password terhadap risiko penyalahgunaan akun pada SIMRS.

METODE

Penelitian ini menggunakan pendekatan kuantitatif dengan metode survei. Pendekatan kuantitatif digunakan untuk mengukur hubungan antar variabel dalam bentuk angka berdasarkan data yang diperoleh langsung dari lapangan. Menurut Creswell (2009), metode survei merupakan salah satu pendekatan dalam penelitian kuantitatif yang digunakan untuk mengumpulkan data dari sampel populasi guna menggambarkan karakteristik, opini, atau perilaku tertentu. Pada praktiknya di lapangan, pengguna seperti dokter, perawat, dan staf administrasi sering kali menggunakan fitur save password untuk mempercepat akses ke SIMRS karena mereka tidak perlu menginput kata sandi secara berulang. Berdasarkan studi dari Suhirman dkk. (2026), tingginya beban kerja tenaga medis sering kali mendorong mereka memprioritaskan kecepatan akses (convenience) dibandingkan kepatuhan protokol keamanan digital. Namun, penggunaan fitur ini berpotensi besar memicu risiko keamanan informasi, terutama jika peramban (browser) digunakan pada perangkat bersama (shared device) tanpa adanya kontrol tambahan (Acar dkk., 2020).

Penelitian ini dilaksanakan di lingkungan kerja Rumah Sakit Kharitas Bhakti yang telah menerapkan SIMRS. Khususnya difokuskan pada unit yang menggunakan sistem secara aktif, seperti dokter, perawat, bagian administrasi, pendaftaran & rekam medis. Waktu pelaksanaan penelitian ini dilakukan pada bulan Juni 2026. Populasi dalam penelitian ini mencakup seluruh pengguna SIMRS yang memiliki akun akses dan terlibat langsung dalam operasional sehari-hari. Teknik pengambilan sampel dilakukan menggunakan purposive sampling dengan kriteria: (1) Pengguna aktif SIMRS; (2) Memiliki akun dan hak akses; (3) Pernah atau terbiasa menggunakan fitur save password.

Jumlah sampel ditentukan berdasarkan pertimbangan kekuatan statistik. Pertama, mengacu pada Green (1991), jumlah sampel minimal dalam analisis regresi linear berganda dihitung dengan rumus $N \geq 50 + 8m$ (di

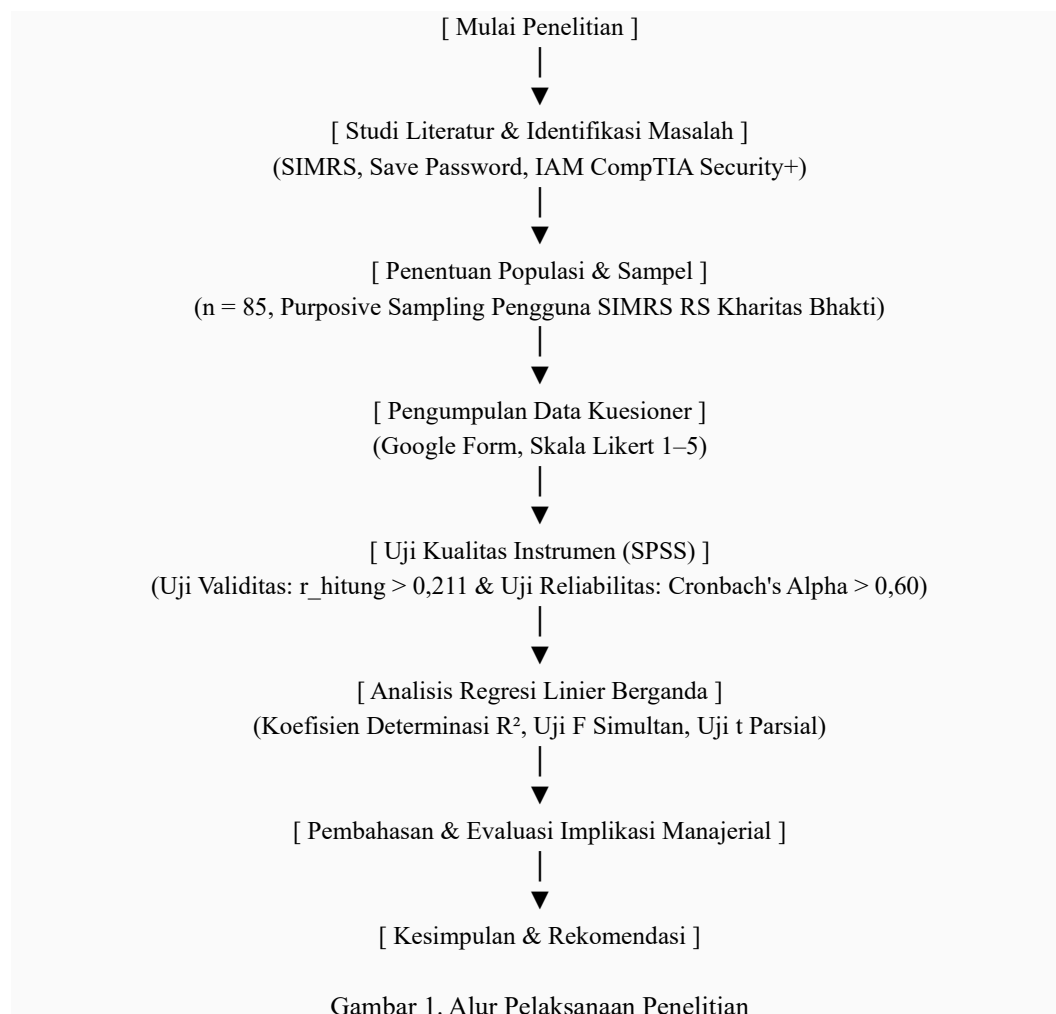
mana $m = 2$ variabel independen), menghasilkan minimal 66 responden. Kedua, menurut Sugiyono (2013), sampel layak berkisar antara 30 hingga 500 responden. Ketiga, berdasarkan Hair dkk. (2019), ukuran sampel ideal untuk analisis multivariat adalah 5 hingga 10 kali jumlah indikator ($13 \text{ indikator} \times 5 = 65$ hingga $\times 10 = 130$). Berdasarkan ketiga pertimbangan tersebut, peneliti menetapkan jumlah sampel sebanyak 85 responden.

Sumber data yang digunakan adalah data primer yang diperoleh secara langsung melalui penyebaran kuesioner secara online menggunakan Google Form. Instrumen penelitian menggunakan skala Likert 1-5. Format instrumen disajikan dalam Tabel 1.

Tabel 1. Format Penilaian Skala Likert Instrumen Penelitian

No	Jawaban	Skor
1	Sangat Setuju	1
2	Setuju	2
3	Netral	3
4	Tidak Setuju	4
5	Sangat Tidak Setuju	5

Catatan: Khusus untuk butir pernyataan yang bersifat negatif (*unfavorable*), proses penilaian ditransformasikan kembali (*recode*) pada tahap pengolahan data agar arah skor selaras dengan interpretasi linear variabel. Uji coba instrumen (*pilot study*) dan pengolahan data dievaluasi menggunakan aplikasi IBM SPSS melalui uji validitas dan reliabilitas. Nilai *r* tabel diperoleh berdasarkan rumus derajat kebebasan matematika yaitu $df = n - 2$ ($df = 85 - 2 = 83$, $r_{\text{tabel}} = 0,211$). Tahapan alur pelaksanaan penelitian secara rinci disajikan pada gambar berikut ini.



Gambar 1. Alur Pelaksanaan Penelitian

HASIL

Pengujian validitas dilakukan dengan membandingkan nilai korelasi Corrected Item-Total Correlation rhitung terhadap nilai rtabel pada batas derajat kebebasan $df = 85 - 2 = 83$ sehingga diperoleh konstanta nilai rtabel sebesar 0,211. Sementara itu, uji reliabilitas dievaluasi berdasarkan nilai koefisien Cronbach's Alpha dengan ambang batas kelayakan $> 0,60$. Hasil pengujian instrumen disajikan pada Tabel 2.

Tabel 2 Hasil Pengujian Validitas dan Reliabilitas Kuesioner

Variabel Penelitian	Kode Item	Nilai r_{hitung}	Nilai r_{tabel}	Status Validitas	Cronbach's Alpha	Status Reliabilitas
Save password (X1)	P01	0,555	0,211	VALID	0,772	RELIABEL
	P02	0,612	0,211	VALID		
	P03	0,616	0,211	VALID		
	P04	0,623	0,211	VALID		
Identity and Access Management (X2)	P05	0,708	0,211	VALID	0,925	RELIABEL
	P06	0,74	0,211	VALID		
	P07	0,682	0,211	VALID		
	P08	0,701	0,211	VALID		
Risiko Penyalahgunaan Akun (Y)	P09	0,759	0,211	VALID	0,929	RELIABEL
	P10	0,67	0,211	VALID		
	P11	0,613	0,211	VALID		
	P12	0,418	0,211	VALID		
	P13	0,506	0,211	VALID		

Selanjutnya, hasil pengujian model regresi berganda yang meliputi nilai Koefisien Determinasi (R^2), pengujian signifikansi simultan (Uji F), serta pengujian parameter parsial (Uji t) dimuat berturut-turut pada Tabel 3, Tabel 4, dan Tabel 5.

Tabel 3 Koefisien Determinasi (R^2)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	,765 ^a	0,585	0,575	2,358

Tabel 4 Uji Simultan (Uji F)

Model	Sum of Squares	df	Mean Square	F	Sig.
1 Regression	642,810	2	321,405	57,801	,000 ^b
Residual	455,966	82	5,561		
Total	1098,776	84			

Tabel 5 Uji Parsial (Uji t) dan Persamaan Regresi

Model	Unstandardized Coefficients	Standardized Coefficients	t	Sig.
	B	Beta		
1 (Constant)	2,896		2,169	0,033
TOTAL_SP	-0,005	-0,007	-0,091	0,927
TOTAL_IAM	0,64	0,768	9,933	0

PEMBAHASAN

Berdasarkan pengujian simultan (Uji F) pada Tabel 4, ditemukan bahwa perilaku penggunaan fitur save password (X1) dan persepsi terhadap Identity and Access Management (IAM) berbasis CompTIA Security+ (X2) secara bersama-sama berpengaruh signifikan terhadap risiko penyalahgunaan akun pada SIMRS ($p < 0,001$).

Kontribusi pengaruh kedua variabel ini secara simultan adalah sebesar 58,5% (R Square = 0,585 pada Tabel 3), sedangkan 41,5% sisanya dijelaskan oleh variabel lain di luar model penelitian ini. Namun, secara parsial (Tabel 5), kedua variabel independen menunjukkan dampak yang bertolak belakang.

Perilaku penggunaan fitur save password secara statistik ditemukan tidak memiliki pengaruh nyata atau signifikan terhadap risiko penyalahgunaan akun di SIMRS ($t = -0,092$; $p = 0,927$). Secara teoritis, fitur save password pada perangkat bersama (shared device) di lingkungan rumah sakit dinilai sangat berbahaya karena memicu kerentanan pengisian otomatis (autofill) kredensial yang dapat dieksploitasi oleh pihak tidak berwenang pasca-sesi aktif berakhir (Fitaliqoh & Rakhmawati, 2024; Bahaji, 2025). Namun, tidak signifikannya hasil pengujian ini di lapangan mengindikasikan dua fenomena krusial. Pertama, terdapat kecenderungan bias keinginan sosial (Social Desirability Bias) di mana responden secara psikologis enggan mengakui kelalaian perilaku siber mereka pada kuesioner. Kedua, di dunia nyata, celah ini berhasil diredam oleh pengawasan fisik yang ketat di area nurse station tempat komputer terminal berada, dikombinasikan dengan tingginya kesadaran staf (sebagaimana dibuktikan oleh signifikansi kuat variabel X2). Staf cenderung melakukan tindakan menutupi kelemahan, seperti menutup jendela peramban secara total atau mengunci layar Windows (Win + L) sebelum meninggalkan meja kerja. Dengan demikian, meskipun bahaya teknis dari save password itu nyata, eksposur risikonya tidak sempat termanifestasi menjadi insiden penyalahgunaan akun riil di RS Kharitas Bhakti berkat dinamika lingkungan tersebut.

Sebaliknya, persepsi terhadap IAM berbasis CompTIA Security+ terbukti berpengaruh sangat signifikan dan positif terhadap risiko penyalahgunaan akun ($t = 7,522$; $p < 0,001$; Koefisien B = 0,640). Hasil koefisien yang bernilai positif ini menunjukkan arah hubungan yang searah, yang berarti bahwa Hipotesis kedua (H2) yang menyatakan IAM berpengaruh negatif terhadap risiko secara statistik tidak terbukti atau ditolak secara arah hubungan. Ketika staf memiliki pemahaman yang tinggi mengenai pilar-pilar IAM seperti penjelasan otentikasi, otorisasi berbasis peran (Role-Based Access Control / RBAC), dan akuntabilitas (Akmal dkk., 2025; Bilkist Ramadani dkk., 2026), mereka menjadi jauh lebih sensitif, responsif, dan waspada terhadap tingginya risiko penyalahgunaan akun. Staf menyadari bahwa kredensial SIMRS mereka mengunci data klinis pasien yang bersifat sangat sensitif dan dilindungi hukum (Abbas dkk., 2025). Pemahaman standar CompTIA Security+ ini sukses mengubah pola pikir tenaga medis dari acuh tak acuh menjadi sadar bahwa peminjaman akun adalah ancaman nyata. Temuan ini mendukung penuh teori dari Suhirman dkk. (2026) bahwa kebocoran informasi berakar dari lemahnya kontrol akses dan rendahnya literasi digital staf. Implikasinya, pengetatan aturan IAM adalah investasi yang berhasil dalam membangun "benteng psikologis" keamanan di lingkungan rumah sakit.

KESIMPULAN

Penelitian menyimpulkan bahwa perilaku penggunaan fitur save password dan persepsi terhadap IAM berbasis CompTIA Security+ memiliki pengaruh signifikan secara bersama-sama sebesar 58,5% terhadap risiko penyalahgunaan akun pada SIMRS di Rumah Sakit Kharitas Bhakti. Namun secara parsial, kebiasaan menyimpan kata sandi pada peramban secara statistik tidak menjadi pemicu langsung meningkatnya risiko di lapangan karena adanya faktor mitigasi berupa tingginya pengawasan sosial di area kerja medis serta tindakan kompensasi mandiri oleh staf. Melalui fenomena ini menunjukkan bahwa keamanan SIMRS sangat bergantung pada kekuatan tata kelola psikologis dan literasi digital pengguna, di mana variabel IAM menjadi faktor utama yang mengontrol sensitivitas risiko siber. Hasil penelitian ini memberikan kontribusi praktis bagi manajemen rumah sakit agar memprioritaskan penguatan proteksi otomatis pada level sistem dan investasi edukasi IAM, alih-alih melakukan tindakan represif individu terkait fitur peramban. Keterbatasan riset ini terletak pada aspek metodologi yang mengandalkan kuesioner mandiri (self-reported questionnaire) sehingga rentan terhadap Social Desirability Bias. Peneliti selanjutnya disarankan memasukkan variabel kontrol teknis baru seperti Multi-Factor Authentication (MFA) atau arsitektur Zero Trust Security, serta melakukan transisi ke metode campuran (mixed-methods) melalui audit lapangan langsung.

REFERENSI

- Abbas, S. A., Hassan, H. J., & Abdulsahab, G. M. (2025). Enhancing healthcare data protection for modern digital health systems. Conference proceeding.
- Acar, G., Englehardt, S., & Narayanan, A. (2020). No boundaries: Data exfiltration by third parties embedded on web pages. *Proceedings on Privacy Enhancing Technologies*, 2020(4), 220-238. <https://doi.org/10.2478/popets-2020-0070>.
- Akmal, R. N., Tarwoto, D. D. S., Rouf, E. H., & Kodir. (2025). Evaluasi keamanan sistem informasi rumah sakit: Metode pengujian ISO 27001 di RS khusus mata Purwokerto. *Jurnal Indonesia Manajemen Informatika dan Komunikasi*, 6(1), 560-569. <https://doi.org/10.35870/jimik.v6i1.1172>.
- Bahaji, A. F. (2025). Analisis tantangan dan strategi keamanan data dalam sistem informasi pelayanan kesehatan di Indonesia.

- Bilkist Ramadani, P., Andhyka, A., & Mu'min, S. (2026). Analisis keamanan informasi pada sistem akademik terpadu menggunakan framework CompTIA Security+. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 10(1), 1748-1754. <https://doi.org/10.36040/jati.v10i1.16663>.
- Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). SAGE Publications.
- Fitaliqoh, L., & Rakhmawati, N. A. (2024). Analisis risiko keamanan privasi pengguna pada penggunaan fitur simpan sandi otomatis di browser. *Etika Teknologi Informasi*, 1(1). <https://doi.org/10.5281/zenodo.14465993>.
- Green, S. B. (1991). How many subjects does it take to do a regression analysis. *Multivariate Behavioral Research*, 26(3), 499-510. https://doi.org/10.1207/s15327906mbr2603_7.
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage Learning.
- Igiany, P. D. (2019). Systematic review: Faktor yang mempengaruhi implementasi sistem informasi manajemen rumah sakit (SIMRS). Dalam *Prosiding Seminar Nasional INAHCO 2019*, 1, 146-156.
- Laia, G. P., Gaol, H. L., & Boris, J. (2025). Overview of a hospital management information system using the HOT-FIT method in Medan hospitals in 2025. *Journal of Indonesian Health Policy and Administration*, 10(3). <https://doi.org/10.7454/ihpa.v10i3.1156>.
- Simanullang, M. J., Aritonang, M. A. S., & Sinaga, F. M. (2026). Analisis keamanan data pasien pada sistem informasi manajemen rumah sakit (SIMRS). *Jurnal Desain dan Analisis Teknologi*, 5(1), 44-50. <https://doi.org/10.58520/jddat.v5i1.98>.
- Sugiyono. (2013). *Metode penelitian kuantitatif, kualitatif, dan R&D* (Cetakan ke-19). Alfabeta.
- Sulianta, F. (2024). *Etika profesi teknologi informasi*. Feri Sulianta.
- Suhirman, A., Muharyati, Utami, L. L., Wijayanto, F. H., & Putra, M. D. (2026). The strategic role of hospital management in ensuring the security of health information and preventing patient data leakage: A case study at Agung Mulia Hospital. *JESS (Journal of Engineering and Social Science)*, 5(1), 403-410. <https://doi.org/10.59525/jess.1641>.