fisip.publiccorner@wiraraja.ac.id
ejournalwiraraja.com

Vol 20, nomor 2, Desember 2025
ISSN 2443-0714 E-ISSN 2621-475X

Analisis Tantangan Keamanan Data dan Privasi dalam Adopsi Aplikasi Kesehatan Digital di Indonesia

Analysis of Data Security and Privacy Challenges in Digital Health App Adoption in Indonesia

Oleh:
Abim Sastrawan
Studi Ilmu Pemerintahan, Fakultas Ilmu Sosial dan Politik, Universitas Muhammadiyah Yogyakarta
E-mail: abimsastrawan@gmail.com

Abstract

Digital health applications offer significant potential for improving healthcare access and efficiency, but their widespread adoption raises major concerns regarding data security and privacy, especially with the utilization of health big data. These applications collect and process highly sensitive information, such as health history and biometrics, making them attractive targets for cyber threats like identity theft and fraud. This study aims to analyze the key data security and privacy challenges in digital health adoption with a focus on big data utilization. Employing a descriptive qualitative method, secondary data from academic literature and regulations were analyzed through thematic content analysis. Findings reveal major vulnerabilities, including weak technical protection, low regulatory compliance, and minimal user awareness of digital risks. Big data is identified as both a risk and a mitigation tool, depending on its ethical management. The conclusion emphasizes that strengthening digital literacy and regulatory enforcement (e.g., UU PDP No. 27/2022) are crucial for building public trust in digital health technology adoption. Further research using mixed-method approaches is recommended for deeper empirical insights.

Keywords*: Digital health, Big data, Data privacy, Data security*

Abstrak

Aplikasi kesehatan digital menawarkan potensi yang signifikan untuk meningkatkan akses dan efisiensi perawatan kesehatan, tetapi adopsi mereka yang luas menimbulkan kekhawatiran besar mengenai keamanan dan privasi data, terutama dengan pemanfaatan big data kesehatan. Aplikasi ini mengumpulkan dan memproses informasi yang sangat sensitif, seperti riwayat kesehatan dan biometrik, menjadikannya target yang menarik untuk ancaman dunia maya seperti pencurian identitas dan penipuan. Studi ini bertujuan untuk menganalisis tantangan keamanan dan privasi data utama dalam adopsi kesehatan digital dengan fokus pada pemanfaatan big data. Dengan menggunakan metode kualitatif deskriptif, data sekunder dari literatur akademik dan regulasi dianalisis melalui analisis konten tematik. Temuan mengungkapkan kerentanan utama, termasuk perlindungan teknis yang lemah, kepatuhan terhadap peraturan yang rendah, dan kesadaran pengguna yang minimal akan risiko digital. Big data diidentifikasi sebagai alat risiko dan mitigasi, tergantung pada manajemen etisnya. Kesimpulan tersebut menekankan bahwa penguatan literasi digital dan penegakan regulasi (misalnya, UU PDP No. 27/2022) sangat penting untuk membangun kepercayaan publik terhadap adopsi teknologi kesehatan digital. Penelitian lebih lanjut menggunakan pendekatan metode campuran direkomendasikan untuk wawasan empiris yang lebih dalam

Kata kunci: Kesehatan digital, Big data, Privasi data, Keamanan data

Vol 20, nomor 2, Desember 2025
ISSN 2443-0714 E-ISSN 2621-475X

1. PENDAHULUAN

Aplikasi kesehatan digital (aplikasi kesehatan) adalah alat potensial untuk meningkatkan aksesibilitas, efisiensi, dan personalisasi perawatan kesehatan (Kartika et al., 2024). Aplikasi yang berisi berbagai fungsi mulai dari pemantauan kebugaran hingga manajemen penyakit kronis, menghasilkan sejumlah besar data. Data ini, yang biasa disebut sebagai "*big data*" kesehatan, memiliki potensi besar untuk mendorong inovasi dalam diagnosis, pengobatan, pencegahan penyakit, dan penelitian kesehatan masyarakat (Sudrajat et al., 2020). Transformasi layanan kesehatan digital tidak dapat dilepaskan dari kerangka kebijakan publik dan tata kelola pemerintahan digital. Penggunaan aplikasi kesehatan oleh pemerintah menuntut adanya regulasi yang jelas, akuntabilitas institusional, serta perlindungan hak warga negara sebagai pengguna layanan publik digital (Pratama, 2021; Sari & Nugroho, 2020). Namun, adopsi aplikasi kesehatan yang meluas bukannya tanpa tantangan. Salah satu kendala utama adalah kekhawatiran tentang keamanan dan privasi data. Aplikasi perawatan kesehatan mengumpulkan dan memproses informasi sensitif, termasuk data demografis, riwayat kesehatan, data biometrik, dan informasi gaya hidup (Djafar, 2019). Data ini sangat berharga bagi peretas dan penjahat dunia maya, yang dapat menggunakannya untuk pencurian identitas, penipuan asuransi, atau pemerasan. Selain itu, pengungkapan informasi kesehatan yang tidak sah dapat merusak reputasi seseorang, meneror diskriminasi, atau memicu tekanan psikologis (Yusilbet, Fauzi, Amanda, Fajrina, Niyar, 2024). Kekhawatiran tentang keamanan dan privasi data diperparah oleh beberapa faktor.

Pertama, banyak aplikasi kesehatan dirancang dengan langkah-langkah keamanan yang tidak memadai, membuatnya rentan terhadap serangan siber. Kedua, peraturan dan standar privasi data kesehatan bervariasi di seluruh negara dan wilayah, sehingga sulit bagi pengembang aplikasi untuk memastikan kepatuhan (Mikraj & Fauzi, 2024) . Ketiga, pengguna sering kali tidak menyadari risiko keamanan dan privasi yang terkait dengan penggunaan aplikasi kesehatan, dan mungkin tidak mengambil tindakan yang tepat untuk melindungi data mereka. Analitik big data memainkan peran penting dalam mengatasi tantangan keamanan data dan privasi dalam adopsi aplikasi layanan kesehatan (Sulistyawati, 2024). Dengan menganalisis data dalam jumlah besar yang dihasilkan oleh aplikasi kesehatan, dimungkinkan untuk mengidentifikasi pola dan anomali yang dapat mengindikasikan pelanggaran keamanan atau pelanggaran privasi. Misalnya, analitik big data dapat digunakan untuk mendeteksi aktivitas yang

Vol 20, nomor 2, Desember 2025
ISSN 2443-0714 E-ISSN 2621-475X

mencurigakan, seperti upaya akses tidak sah atau transfer data yang tidak biasa. Ini juga dapat digunakan untuk mengidentifikasi aplikasi kesehatan yang mengumpulkan atau berbagi data secara tidak sah (Eka Mayasari & Agussalim Agussalim, 2023).

Meskipun banyak penelitian telah dilakukan tentang keamanan siber dalam konteks teknologi informasi, ada kesenjangan penelitian yang signifikan dalam konteks aplikasi kesehatan digital. Penelitian oleh Punithavathi & Subbiah (2022) menunjukkan bahwa meskipun ada banyak penelitian tentang keamanan data di sektor lain seperti perbankan dan e-commerce, hanya sedikit yang secara khusus membahas tantangan unik yang dihadapi oleh aplikasi kesehatan digital. Selain itu, penelitian lain menemukan bahwa kebijakan privasi yang ada seringkali tidak cukup untuk melindungi data sensitif pengguna, sehingga menciptakan kesenjangan antara praktik terbaik dan implementasi nyata di lapangan (Oku et al., 2022). Hal ini menunjukkan perlunya analisis yang lebih mendalam tentang tantangan spesifik yang dihadapi oleh aplikasi kesehatan digital dalam hal keamanan dan privasi data. Selain itu, analitik big data dapat digunakan untuk meningkatkan keamanan dan privasi aplikasi Perawatan Kesehatan (Indriyajati et al., 2023). Misalnya, dapat digunakan untuk mengembangkan algoritme pembelajaran mesin yang dapat mendeteksi dan mencegah serangan siber. Ini juga dapat digunakan untuk membuat sistem manajemen privasi yang lebih efektif yang memungkinkan pengguna mengontrol bagaimana data mereka dikumpulkan, digunakan, dan dibagikan. Mengingat potensi manfaat dan risiko yang terkait dengan adopsi aplikasi kesehatan, sangat penting untuk mengatasi tantangan keamanan dan privasi data (Zhu et al., 2020).

Tujuan dari penelitian ini adalah untuk menganalisis tantangan utama terkait keamanan dan privasi data dalam adopsi aplikasi kesehatan digital dengan fokus pada big data. Penelitian ini bertujuan untuk mengidentifikasi faktor risiko yang berkontribusi terhadap pelanggaran privasi serta mengevaluasi efektivitas langkah-langkah mitigasi yang saat ini diterapkan oleh pengembang aplikasi.

Kontribusi penelitian ini ada dua; Secara teoritis, hasil penelitian diharapkan dapat memperkaya literatur tentang keamanan siber dengan memberikan wawasan baru tentang tantangan spesifik dalam konteks aplikasi kesehatan digital. Secara praktis, temuan penelitian ini dapat dijadikan panduan bagi pengembang aplikasi dan pembuat kebijakan untuk merumuskan strategi yang lebih efektif dalam melindungi data pengguna dan meningkatkan kepercayaan masyarakat terhadap penggunaan teknologi di sektor kesehatan. Dengan demikian, penelitian

Vol 20, nomor 2, Desember 2025
ISSN 2443-0714 E-ISSN 2621-475X

ini tidak hanya relevan secara akademis tetapi juga memiliki implikasi langsung bagi praktik industri.

2. TINJAUAN TEORITIS

Dalam konteks adopsi aplikasi kesehatan digital, tantangan keamanan dan privasi data telah menjadi fokus utama dalam berbagai penelitian. Serangan siber di sektor perawatan kesehatan meningkat secara signifikan, dengan data pasien menjadi target utama, sehingga membutuhkan solusi yang efektif untuk melindungi informasi sensitive (Besenyő & Kovács, 2023). Esmaeilzadeh (2019) menekankan pentingnya transparansi dalam kebijakan privasi untuk membangun kepercayaan pengguna terhadap aplikasi kesehatan digital, yang merupakan faktor kunci dalam adopsi teknologi ini.

Dalam perspektif administrasi publik, penerapan teknologi digital dalam pelayanan publik harus disertai dengan tata kelola yang adaptif, transparan, dan terintegrasi lintas sektor. Lemahnya koordinasi kebijakan dan fragmentasi regulasi sering menjadi kendala utama dalam implementasi e-government di sektor pelayanan publik, termasuk sektor kesehatan (Hidayat, 2022). Mavriki & Karyda (2020) mengeksplorasi bagaimana analitik big data dapat digunakan untuk meningkatkan keamanan dan privasi dalam aplikasi perawatan kesehatan, menunjukkan bahwa penggunaan big data dapat membantu mendeteksi ancaman sejak dini. Pilla (2023) memberikan analisis mendalam tentang pelanggaran data yang terjadi di sektor perawatan kesehatan, serta dampaknya terhadap privasi pasien, yang menunjukkan perlunya tindakan pencegahan yang lebih ketat. Selain itu, Ranjani & Jeyamala (2020) membahas penerapan algoritme pembelajaran mesin dalam mendeteksi ancaman keamanan dalam aplikasi perawatan kesehatan, menyoroti potensi teknologi ini dalam meningkatkan sistem keamanan. Selain itu, penelitian lainnya meneliti tentang kekhawatiran pengguna mengenai privasi data di aplikasi kesehatan digital, menunjukkan bahwa persepsi pengguna sangat memengaruhi adopsi aplikasi tersebut (Saad et al., 2020).

Surridge (2019) membahas berbagai kerangka peraturan yang ada untuk melindungi data kesehatan di seluruh dunia, menekankan pentingnya kepatuhan terhadap peraturan untuk menjaga keamanan data. Abouelmehdi (2018) mengeksplorasi bagaimana big data dapat digunakan untuk meningkatkan keselamatan dan privasi pasien, menunjukkan bahwa analisis data yang tepat dapat memberikan wawasan yang berharga. El Ouazzani (2021) memberikan gambaran tentang tantangan yang dihadapi dalam menjaga keamanan data dalam aplikasi kesehatan digital, yang mencakup masalah teknis dan non-teknis. Terakhir, Chang (2022) membahas implikasi etis dari

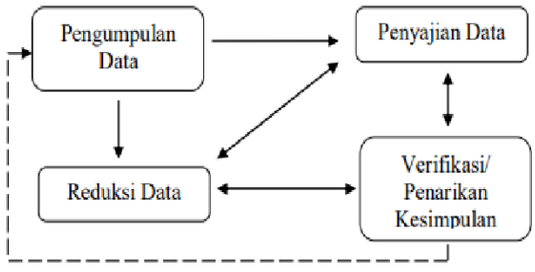
Vol 20, nomor 2, Desember 2025
ISSN 2443-0714 E-ISSN 2621-475X

penggunaan big data dalam perawatan kesehatan, dengan fokus pada keseimbangan antara inovasi dan perlindungan privasi, yang semakin relevan di era digital saat ini.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif untuk menganalisis tantangan privasi dan keamanan dalam adopsi aplikasi kesehatan digital, dengan fokus khusus pada penggunaan big data. Pendekatan ini dipilih karena mampu menggambarkan secara mendalam dan kontekstual bagaimana isu privasi dan keamanan berkembang seiring dengan meningkatnya penggunaan big data di sektor kesehatan digital (Raj et al., 2022). Data yang digunakan bersifat sekunder, dikumpulkan dari berbagai sumber terpercaya seperti artikel jurnal ilmiah, laporan lembaga internasional misalnya World Health Organisation (WHO), peraturan pemerintah, dan dokumen teknis dari pengembang aplikasi Kesehatan. Kriteria pemilihan data meliputi publikasi yang diterbitkan pada periode 2020 hingga 2024, berfokus pada keamanan data, privasi, dan big data dalam sistem kesehatan digital, serta berasal dari sumber yang diverifikasi secara akademis atau kelembagaan (Li et al., 2021).

Pengumpulan data dilakukan melalui pencarian sistematis di database seperti Scopus, ScienceDirect, dan Google Scholar, menggunakan kata kunci seperti "big data in digital health", "data privacy in mHealth", dan "cybersecurity in healthcare applications" (Al-Muhtadi et al., 2019). Data yang diperoleh dianalisis menggunakan metode analisis konten, yaitu dengan mengidentifikasi pola tematik, isu utama, dan hubungan antar variabel seperti regulasi, teknologi, dan perilaku pengguna. Untuk menjaga validitas, triangulasi sumber dilakukan dengan membandingkan berbagai jenis publikasi dan perspektif dari peneliti yang berbeda (Gurr & Metag, 2022). Hasil analisis ini diharapkan dapat memberikan wawasan yang komprehensif tentang tantangan dan risiko privasi yang timbul akibat integrasi big data dalam aplikasi kesehatan digital, serta memberikan landasan teoritis dan praktis bagi pengembangan strategi perlindungan data di era transformasi digital Kesehatan



Gambar 1. Aliran Model Analisis Data Kualitatif

Sumber: Ibad et al., (2022)

Vol 20, nomor 2, Desember 2025
ISSN 2443-0714 E-ISSN 2621-475X

4. HASIL DAN PEMBAHASAN

Tantangan signifikan terkait keamanan dan privasi data dalam adopsi aplikasi kesehatan digital

Indikator	Temuan Utama	Dampak	Sumber
Keamanan teknis	Tidak diterapkannya enkripsi end-to-end dan autentikasi ganda	Kebocoran data dan akses ilegal	Jarecki et al. (2021)
Kepatuhan regulasi	Regulasi kesehatan digital belum terintegrasi lintas sektor	Perlambatan pengembangan aplikasi	Liu et al. (2020)
Kesadaran pengguna	Pengguna tidak membaca kebijakan privasi	Tingginya risiko penyalahgunaan data	Saad et al. (2020)

Tabel 1. Temuan Utama Tantangan Keamanan dan Privasi Data Aplikasi Kesehatan Digital

1. Keamanan Lemah

Keamanan lemah menjadi perhatian utama karena banyak aplikasi tidak memiliki perlindungan teknis yang memadai. Misalnya, masih banyak aplikasi yang belum menerapkan enkripsi end-to-end atau sistem autentikasi dua faktor. Ketiadaan perlindungan ini membuka celah bagi pihak ketiga untuk mengakses data pribadi pasien, yang dapat menimbulkan kebocoran informasi sensitif dan pelanggaran privasi (Jarecki et al., 2021).

2. Kepatuhan Peraturan Rendah

Kepatuhan terhadap peraturan yang rendah juga menjadi hambatan signifikan. Hal ini disebabkan oleh tidak adanya standar global yang seragam dalam regulasi data kesehatan digital. Akibatnya, pengembang aplikasi sering kali kesulitan untuk mematuhi berbagai peraturan yang berlaku di tingkat lokal maupun internasional secara bersamaan. Ketidakkonsistenan regulasi ini dapat memperlambat pengembangan teknologi serta membingungkan pemangku kepentingan dalam hal kewajiban hukum dan etika (Liu et al., 2020). Sebagai contoh, kasus aplikasi PeduliLindungi menunjukkan adanya tumpang tindih kewenangan antara Kementerian Kesehatan, Kominfo, dan pengelola platform digital terkait pengelolaan, penyimpanan, serta pemanfaatan data pengguna. Perbedaan standar pengelolaan data sebelum dan sesudah berlakunya UU PDP No. 27 Tahun 2022 menyebabkan ketidakpastian hukum bagi pengembang aplikasi, khususnya dalam hal retensi data dan hak subjek data, sehingga memperlambat optimalisasi sistem dan integrasi layanan kesehatan digital (Lestari & Putra, 2023).

3. Kesadaran Pengguna

Tantangan yang tidak kalah penting adalah kesadaran pengguna yang minimal. Banyak pengguna aplikasi kesehatan digital yang belum memahami secara menyeluruh risiko yang melekat dalam penggunaan teknologi ini, seperti kemungkinan

Vol 20, nomor 2, Desember 2025
ISSN 2443-0714 E-ISSN 2621-475X

penyalahgunaan data atau kurangnya transparansi pengelolaan informasi. Rendahnya kesadaran pengguna terhadap kebijakan privasi tidak hanya disebabkan oleh faktor individu, tetapi juga dipengaruhi oleh lemahnya transparansi pemerintah dalam mengomunikasikan kebijakan pengelolaan data publik. Dalam konteks pelayanan publik digital, kepercayaan publik menjadi faktor kunci keberhasilan implementasi sistem berbasis teknologi (Wicaksono, 2021). Rendahnya literasi digital dan privasi menyebabkan pengguna cenderung mengabaikan izin akses aplikasi tanpa membaca ketentuan secara cermat, sehingga memperbesar potensi risiko privasi (Saad et al., 2020).

Peran Big Data dalam Mendukung Keamanan Aplikasi Kesehatan Digital

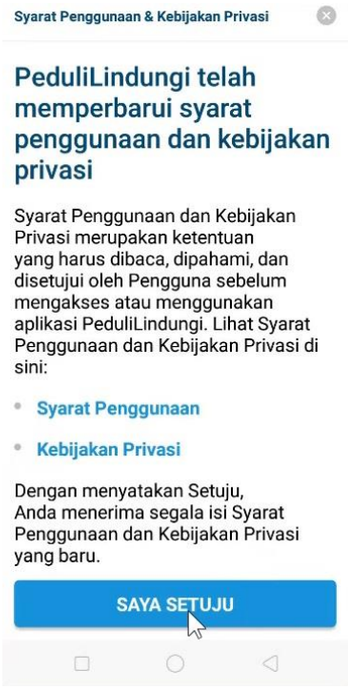
Pemanfaatan big data dalam dunia kesehatan digital memberikan kontribusi yang signifikan, terutama dalam hal penguatan sistem keamanan (Sugiarto & Farid, 2023). Melalui teknologi ini, penyedia layanan kesehatan dapat langsung memantau pergerakan data dan pola perilaku pengguna dengan bantuan algoritme yang dirancang untuk mengenali aktivitas yang mencurigakan. Misalnya, sistem dapat mendeteksi lonjakan upaya login dari lokasi atau perilaku yang tidak biasa yang menyimpang dari kebiasaan pengguna, yang dapat menjadi indikator ancaman dunia maya (Kumar & Sharma, 2023). Penggunaan big data memungkinkan tindakan pencegahan yang lebih aktif terhadap berbagai bentuk serangan digital, termasuk pencurian data, intrusi sistem, dan serangan ransomware. Sistem analitik ini mampu menyaring informasi dalam jumlah besar dan menghasilkan prediksi potensi risiko, sehingga penyedia layanan dapat mengambil tindakan sebelum kerugian yang lebih serius terjadi (Ahmad et al., 2022).

Perlindungan Privasi Melalui Analisis Data yang Bertanggung Jawab

Selain menjadi alat pendeteksi ancaman keamanan, big data juga membantu penyedia layanan kesehatan dalam menjaga privasi data pengguna (Sulistyawati, 2024). Dengan mempelajari bagaimana data dikumpulkan dan digunakan, manajer dapat mengidentifikasi titik lemah dalam sistem dan merancang strategi perlindungan data yang lebih komprehensif dan terbuka. Kebijakan privasi yang dibuat dengan pendekatan ini biasanya lebih mampu beradaptasi dengan dinamika penggunaan teknologi, serta menciptakan rasa aman di antara pengguna (Hasminiar et al., 2024). Namun, menjaga kerahasiaan identitas individu tetap menjadi tantangan. Untuk menjamin bahwa data yang dianalisis tidak membahayakan privasi pengguna, perlu menerapkan metode seperti *Anonimitisasi* yaitu menghapus informasi identitas dari data atau *Nama samaran*, yaitu mengganti data identitas

Vol 20, nomor 2, Desember 2025
ISSN 2443-0714 E-ISSN 2621-475X

dengan kode tertentu (Ome et al., 2024). Teknik-teknik ini memungkinkan analisis berlanjut tanpa mengorbankan hak privasi pengguna. Lebih dari sekadar tindakan teknis, pendekatan ini merupakan bentuk tanggung jawab moral dalam pengelolaan data. Bukti visual mengenai tampilan kebijakan privasi aplikasi kesehatan digital dapat dilihat pada Gambar 1.



Gambar 2. Tampilan Kebijakan Privasi Aplikasi PeduliLindungi
Sumber: Dokumentasi penulis (2025)

Tanggung Jawab Hukum dan Etika dalam Perlindungan Data Pribadi

Dalam praktiknya, semua kegiatan yang berkaitan dengan pengolahan data—khususnya data kesehatan—harus dilakukan sesuai dengan ketentuan hukum yang berlaku. Di Indonesia, peraturan ini tertuang dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang memberikan kerangka hukum perlindungan data individu (Suryanto & Riyanto, 2024). Aturan ini mengharuskan pengontrol data untuk mendapatkan persetujuan dari pemilik data dan memberi mereka hak untuk mengetahui, memperbaiki, atau bahkan menghapus data pribadi mereka. Oleh karena itu, penyedia aplikasi kesehatan digital perlu memastikan bahwa seluruh proses pengumpulan dan analisis data memenuhi standar kepatuhan yang ditetapkan. Data yang dikumpulkan tidak boleh disalahgunakan, dan pengguna harus diberikan akses penuh ke informasi yang berkaitan dengan data mereka. Jika aspek ini diabaikan, tidak hanya konsekuensi hukum yang harus dihadapi, tetapi juga hilangnya kepercayaan publik yang dapat merugikan kredibilitas institusi (Surridge et al., 2019).

Keterlibatan Pengguna Aktif dan Literasi Data sebagai Pilar Kepercayaan

Dalam konteks manajemen data berkelanjutan, keterlibatan pengguna memainkan peran penting. Pengguna aplikasi kesehatan perlu diberikan informasi yang jelas dan mudah dipahami tentang bagaimana data mereka digunakan dan dilindungi (Ilhadi et al., 2024). Proses edukasi ini idealnya dilakukan sejak awal menggunakan aplikasi, sehingga pengguna merasa nyaman dan memiliki

Vol 20, nomor 2, Desember 2025
ISSN 2443-0714 E-ISSN 2621-475X

kendali atas informasi pribadi yang mereka bagikan. Ketika pengguna merasa bahwa mereka terlibat dan diberi kendali atas data mereka sendiri, kepercayaan pada platform meningkat. Kepercayaan ini merupakan fondasi utama dalam membangun sistem digital yang tidak hanya efisien, tetapi juga berkelanjutan dan berorientasi pada kebutuhan manusia. Dengan cara ini, keberadaan teknologi kesehatan digital akan semakin diterima oleh masyarakat luas, karena mampu menciptakan rasa aman sekaligus memberikan manfaat nyata.

5. PENUTUP

Penelitian ini menyoroti bahwa tantangan utama dalam implementasi aplikasi kesehatan digital terletak pada aspek perlindungan data pribadi pengguna yang masih rentan terhadap pelanggaran. Meskipun penggunaan big data dalam aplikasi perawatan kesehatan menawarkan berbagai keuntungan seperti peningkatan efisiensi layanan dan akurasi diagnostik, hal ini juga membuka kesenjangan risiko terhadap kebocoran informasi sensitif. Tiga isu utama yang ditemukan adalah lemahnya perlindungan teknis pada aplikasi, rendahnya kepatuhan terhadap regulasi perlindungan data pribadi, serta minimnya kesadaran pengguna terhadap risiko digital. Pemanfaatan big data di satu sisi memperkuat kemampuan deteksi ancaman siber dan pengelolaan privasi, tetapi di sisi lain dapat meningkatkan potensi pelanggaran jika tidak dikelola secara etis. Dengan demikian, temuan penelitian ini memberikan pemahaman yang relevan tentang tujuan penelitian, yaitu mengidentifikasi risiko privasi dan mengevaluasi efektivitas langkah-langkah mitigasi yang tersedia saat ini. Kontribusi penelitian ini yaitu memperkaya wacana ilmiah secara akademis di bidang keamanan data digital, khususnya dalam konteks aplikasi kesehatan, dan secara praktis memberikan masukan strategis bagi pengembang aplikasi dan pembuat kebijakan untuk memperkuat sistem perlindungan data. Meskipun demikian, penelitian ini memiliki keterbatasan karena mengandalkan data sekunder dan pendekatan kualitatif berbasis literatur, yang membatasi kedalaman analisis empiris serta ruang untuk generalisasi temuan. Kurangnya data primer dari aktor langsung, seperti pengembang atau pengguna aplikasi, menjadi hambatan untuk mendapatkan gambaran yang lebih kontekstual. Oleh karena itu, penelitian lebih lanjut direkomendasikan untuk menggunakan pendekatan campuran, termasuk wawancara mendalam dan analisis sistem keamanan teknis. Penelitian di masa depan juga perlu diarahkan pada pengembangan algoritma berbasis big data adaptif dalam mendeteksi ancaman keamanan dan merancang sistem manajemen privasi yang relevan dengan kondisi lokal.

Vol 20, nomor 2, Desember 2025
ISSN 2443-0714 E-ISSN 2621-475X

DAFTAR PUSTAKA

Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (n.d.). *Big healthcare data: preserving security and privacy. J. Big Data 5 (1)(2018)*.

Ahmad, F., Abidin, S., Qureshi, I., & Ishrat, M. (2022). Big Data and Its Role in Cybersecurity. *International Conference on Innovations in Data Analytics*, 131–144.

Al-Muhtadi, J., Shahzad, B., Saleem, K., Jameel, W., & Orgun, M. A. (2019). Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment. *Health Informatics Journal*, *25*(2), 315–329.

Besenyő, J., & Kovács, A. M. (2023). Healthcare cybersecurity threat context and mitigation opportunities. *Security Science Journal*, *4*(1), 83–101.

Chang, V., Eniola, R. O., Liu, B. S.-C., & Arami, M. (2022). An Ethical Framework for Big Data and Smart Healthcare. *FEMIB*, 65–74.

Djafar, W. (2019). Hukum Perlindungan Data Pribadi di Indonesia: Lanskap Urgensi dan Kebutuhan Pembaruan. *Seminar Hukum Dalam Era Analisis Big Data*, *2013*, 1–14. http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm.

Eka Mayasari, & Agussalim Agussalim. (2023). Literature Review: Big Data dan Data Analys pada Perusahaan. *Jurnal Ilmiah Sistem Informasi Dan Ilmu Komputer*, *3*(3), 171–187. https://doi.org/10.55606/juisik.v3i3.680

El Ouazzani, Z., El Bakkali, H., & Sadki, S. (2021). Privacy preserving in digital health: main issues, technologies, and solutions. In *Research Anthology on Privatizing and Securing Data* (pp. 1503–1526). IGI Global.

Esmaeilzadeh, P. (2019). The impacts of the perceived transparency of privacy policies and trust in providers for building trust in health information exchange: empirical study. *JMIR Medical Informatics*, *7*(4), e14050.

Gurr, G., & Metag, J. (2022). Content analysis in the research field of technology coverage. In *Standardisierte Inhaltsanalyse in der Kommunikationswissenschaft–Standardized Content Analysis in Communication Research: Ein Handbuch-A Handbook* (pp. 239–247). Springer Fachmedien Wiesbaden Wiesbaden.

Hasminiar, H., Hidayat, R., Karyono, O., Fitri, N. A., & Anggryani, L. (2024). Inovasi dalam Model Bisnis Distribusi: Tantangan dan Peluang di Era Digital. *EKOMA : Jurnal Ekonomi, Manajemen, Akuntansi*, *3*(6), 867–880. https://doi.org/10.56799/ekoma.v3i6.4536

Hidayat, M. (2022). Tantangan Implementasi E-Government di Sektor Pelayanan Publik. *Public Corner*, *17*(1), 12–26.

Ibad, S., Farisia, H., Aisyah, P., & Destinasari, B. (2022). Pemahaman Masyarakat Dalam Melakukan Upaya Preventif Penyebaran Covid-19 Melalui Rekonseptualisasi Nilai-Nilai Qada Dan Qadar. *Kanz Philosophia A Journal for Islamic Philosophy and Mysticism*, *8*, 183–206. https://doi.org/10.20871/kpjipm.v8i2.222

Ilhadi, V., Syukriah, S., Rosdiana, R., Asran, A., Asran, A., & Yusuf, E. (2024). Pendampingan Teknologi Informasi Berkelanjutan Dalam Peningkatan Pengembangan Digitalisasi Dibidang Pelayanan Publik Dan Kearsipan. *Jurnal Malikussaleh Mengabdi*, *3*(1), 121. https://doi.org/10.29103/jmm.v3i1.16696

Indriyajati, F., Jawa, M. M. S. D., & Utomo, H. (2023). Analisis Keamanan Data Electronic Medical Record Digital Transformation Office (DTO) Kementerian Kesehatan Indonesia. *Sanskara Manajemen Dan Bisnis*, *2*(01), 59–66. https://doi.org/10.58812/smb.v2i01.130

Jarecki, S., Jubur, M., Krawczyk, H., Saxena, N., & Shirvanian, M. (2021). Two-factor password-authenticated key exchange with end-to-end security. *ACM Transactions on Privacy and Security (TOPS)*, *24*(3), 1–37.

Kartika, R. W., Liem, J. F., & Widjaja, D. (2024). *Penggunaan Ukrida ChatBot pada Pemeriksaan Kesehatan Karyawan Rumah Sakit Ukrida*. 247–258.

Kumar, A., & Sharma, I. (2023). Enhancing

Vol 20, nomor 2, Desember 2025
ISSN 2443-0714 E-ISSN 2621-475X

data privacy of iot healthcare with keylogger attack mitigation. *2023 4th International Conference for Emerging Technology (INCET)*, 1–6.

Lestari, N., & Putra, A. (2023). Keamanan Informasi dalam Sistem Layanan Publik Digital. *Public Corner*, *18*(2), 67–81.

Li, L., Novillo-Ortiz, D., Azzopardi-Muscat, N., & Kostkova, P. (2021). Digital data sources and their impact on people's health: a systematic review of systematic reviews. *Frontiers in Public Health*, *9*, 645260.

Liu, P., Astudillo, K., Velez, D., Kelley, L., Cobbs-Lomax, D., & Spatz, E. S. (2020). Use of mobile health applications in low-income populations: a prospective study of facilitators and barriers. *Circulation: Cardiovascular Quality and Outcomes*, *13*(9), e007031.

Mavriki, P., & Karyda, M. (2020). Big data analytics in healthcare applications: privacy implications for individuals and groups and mitigation strategies. *European, Mediterranean, and Middle Eastern Conference on Information Systems*, 526–540.

Mikraj, A. L., & Fauzi, M. R. (2024). *Tantangan dan Solusi Administrasi Kesehatan di Era Digital (Tinjauan Literature Review atas Implementasi Teknologi)*. *5*(1), 1093–1103.

Oku, R., Shiomoto, K., & Ohba, Y. (2022). Decentralized Identifier and Access Control Based Architecture for Privacy-Sensitive Data Distribution Service. *2022 IEEE 8th World Forum on Internet of Things (WF-IoT)*, 1–6.

Ome, P. J., Adwah, F. D., & Data, K. (2024). *ANONIMISASI DAN PSEUDONIMISASI DATA DALAM SISTEM OPERASI WINDOWS*. *20*(1), 36–43.

Pilla, R., Oseni, T., & Stranieri, A. (2023). A study into the impact of data breaches of electronic health records. In *Proceedings of the 2023 Australasian Computer Science Week* (pp. 252–254).

Pratama, A. B. (2021). Tata Kelola Data Publik dalam Era Digital Governance. *Public Corner*, *16*(1), 45–58.

Punithavathi, P., & Subbiah, G. (2022). Digital Healthcare Security Issues: Is There a Solution in Biometrics? In *Research Anthology on Securing Medical Systems and Records* (pp. 17–30). IGI Global.

Raj, R., Daneshgar, F., & Borhan, N. (2022). Evaluating Challenges in Using Big Data in Healthcare. *Proceedings of Sixth International Congress on Information and Communication Technology: ICICT 2021, London, Volume 1*, 59–69.

Ranjani, J. J., & Jeyamala, C. (2020). Machine learning algorithms for medical image security. In *Intelligent Data Security Solutions for e-Health Applications* (pp. 169–183). Elsevier.

Saad, A., Haridi, H. K., Sulaiman, A., & Alzabni, T. (2020). The Impact of Patients' Trust and Privacy on Use of Medical Mobile Applications. *Innovative Mobile and Internet Services in Ubiquitous Computing: Proceedings of the 13th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-2019)*, 429–436.

Sari, D. P., & Nugroho, R. (2020). Kebijakan Perlindungan Data Pribadi dalam Pelayanan Publik Digital. *Public Corner*, *15*(2), 89–103.

Sudrajat, I., Riza, H., Moehtadi, F., & Panggabean, L. (2020). Peran Iptekin dalam mengatasi COVID-19: pembelajaran dari beberapa negara. *Jurnal Sistem Cerdas*, *3*(2), 112–122. https://doi.org/10.37396/jsc.v3i2.73

Sugiarto, & Farid, A. (2023). Literasi Digital Sebagai Jalan Penguatan Pendidikan Karakter Di Era Society 5.0. *Cetta: Jurnal Ilmu Pendidikan*, *6*(3), 580–597. https://doi.org/10.37329/cetta.v6i3.2603

Sulistyawati, U. S. (2024). *Decoding Big Data : Mengubah Data Menjadi Keunggulan Kompetitif dalam Pengambilan Keputusan Bisnis Abstrak*. *1*(2), 58–71.

Surridge, M., Meacham, K., Papay, J., Phillips, S. C., Pickering, J. B., Shafiee, A., & Wilkinson, T. (2019). Modelling compliance threats and security analysis of cross border health data exchange. *International Conference on Model and Data Engineering*, 180–189.

Suryanto, D., & Riyanto, S. (2024). Tentang Perlindungan Data Pribadi Dalam

Vol 20, nomor 2, Desember 2025
ISSN 2443-0714 E-ISSN 2621-475X

Industri Ritel “ Tinjauan Terhadap Kepatuhan Dan Dampaknya. *Veritas*, *10*(1), 121–135.

Wicaksono, A. (2021). Kepercayaan Publik dalam Transformasi Digital Pemerintahan. *Public Corner*, *16*(2), 101–115.

Yusilbet, Fauzi, Amanda, Fajrina, Niyar, S. (2024). Peran Manajemen Sekuriti Dalam Mencegah Resiko Kerugian Terhadap Keuangan Digital. *Jurnal Kewirausahaan Dan Multi Talenta*, *2*(2), 148–161.

Zhu, S., Saravanan, V., & Muthu, B. A. (2020). Achieving data security and privacy across healthcare applications using cyber security mechanisms. In *Electronic Library* (Vol. 38, Issues 5–6, pp. 979–995). https://doi.org/10.1108/EL-07-2020-0219