

RAISING AWARENESS OF THE MISUSE OF PERSONAL HEALTH DATA ON DIGITAL PLATFORMS/HEALTH APPLICATIONS

SOSIALISASI WASPADA PENYALAHGUNAAN DATA KESEHATAN PRIBADI DI PLATFORM DIGITAL/APLIKASI KESEHATAN

M. Syahputra^{1*}, Imrah Sari², Anita Citra Yeni³, Herman Susilo⁴, Nandra⁵

^{1,2,4} Manajemen Informasi Kesehatan, Universitas Syedza Saintika, Indonesia

³ Bisnis Digital, Universitas Syedza Saintika, Indonesia

⁵ Manajemen Informatika, Politeknik Lembaga Pendidikan dan Pengembangan Profesi Indonesia, Indonesia

Email: ^{1*}syahputra0404@gmail.com

NO WhatsApp Aktiv Penulis (Wajib di isi):

Recieve: 10 September 2026

Reviewed: 17 September 2026

Accepted: 10 Oktober 2026

Abstract: *Digital platforms and health applications provide convenience in accessing information, conducting consultations, monitoring health conditions, and storing health records. However, the increasing exchange of personal health data also creates risks of misuse, data breaches, unauthorized access, tracking, and use for purposes that users do not fully understand. This community service program (PKM) aims to increase public knowledge and awareness of personal health data protection when using digital platforms/health applications. The activity uses an educational-participatory approach through health education sessions, demonstrations of application permissions and privacy policies, discussions, and knowledge evaluation using pre-tests and post-tests. The materials cover types of personal health data, forms of misuse, risk indicators, consent principles, application permission settings, account security, link verification, and incident-reporting procedures. Recent literature indicates that privacy, security, transparency, and user awareness are important factors in safe mHealth use. This activity is expected to improve the community's digital privacy literacy so that users become more critical before providing, storing, or sharing health data through digital applications.*

Keyword: *personal health data; digital privacy; Health; data security; digital literacy*

Abstrak. Platform digital dan aplikasi kesehatan memberikan kemudahan dalam mengakses informasi, melakukan konsultasi, memantau kondisi kesehatan, dan menyimpan rekam kesehatan. Namun, meningkatnya pertukaran data kesehatan pribadi juga menimbulkan risiko penyalahgunaan, kebocoran data, akses tanpa izin, pelacakan (tracking), serta penggunaan data untuk tujuan yang tidak sepenuhnya dipahami pengguna. Program pengabdian kepada masyarakat (PKM) ini bertujuan untuk meningkatkan pengetahuan dan kesadaran masyarakat mengenai perlindungan data kesehatan pribadi saat menggunakan platform digital/aplikasi kesehatan. Kegiatan dilaksanakan dengan pendekatan edukatif-partisipatif melalui sesi edukasi kesehatan, demonstrasi pemeriksaan izin aplikasi dan kebijakan privasi, diskusi, serta evaluasi pengetahuan menggunakan pre-test dan post-test. Materi yang disampaikan mencakup jenis data kesehatan pribadi, bentuk penyalahgunaan, indikator risiko, prinsip persetujuan (consent), pengaturan izin aplikasi, keamanan akun, verifikasi tautan, dan prosedur pelaporan insiden. Literatur terkini menunjukkan bahwa privasi, keamanan, transparansi, dan kesadaran pengguna merupakan faktor penting dalam penggunaan mHealth yang aman.

Kegiatan ini diharapkan dapat meningkatkan literasi privasi digital masyarakat sehingga pengguna menjadi lebih kritis sebelum memberikan, menyimpan, atau membagikan data kesehatan melalui aplikasi digital.

Keyword: data kesehatan pribadi; privasi digital; mHealth; keamanan data; literasi digital

Copyright © 2026, M. Syahputra, Imrah Sari, Anita Citra

Yeni, Herman Susilo, Nandra

doi:10.32528/jhce.v4i3.6556



This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/).

PENDAHULUAN

Transformasi digital di bidang kesehatan telah memperluas penggunaan layanan telehealth, rekam medis elektronik, aplikasi pemantauan kesehatan, perangkat wearable, dan berbagai layanan kesehatan berbasis aplikasi. Perkembangan ini menghasilkan volume data kesehatan yang semakin besar dan bernilai. Data yang dikumpulkan dapat mencakup identitas, riwayat medis, hasil pemeriksaan, informasi pengobatan, data biometrik, lokasi, aktivitas, dan informasi perilaku. Literatur terkini menegaskan bahwa data kesehatan merupakan informasi sensitif yang memerlukan perlindungan kuat karena kebocoran data dapat menimbulkan konsekuensi sosial, hukum, ekonomi, dan psikologis bagi individu (Raab et al., 2023).

Risiko tidak hanya muncul dari serangan siber. Pengguna dapat menghadapi risiko ketika aplikasi meminta izin akses yang tidak relevan, kebijakan privasi sulit dipahami, data dibagikan kepada pihak ketiga, atau pengguna memberikan persetujuan tanpa mengetahui tujuan pemrosesan data. (Rezaee et al., n.d.) mengidentifikasi kriteria keamanan dan privasi mHealth yang penting, meliputi autentikasi, otorisasi, manajemen akses, penyimpanan data, integritas, enkripsi, privasi, dan konten kebijakan privasi. Studi empiris lain menunjukkan bahwa sebagian pengguna cenderung mengabaikan kebijakan privasi dan memberikan izin aplikasi secara berlebihan (Pool et al., 2024).

Dari sisi pengguna, kesadaran merupakan faktor penting. Tinjauan sistematis oleh Nicole et al. (2024) menunjukkan bahwa pengguna memiliki tingkat kepedulian dan pemahaman yang beragam terhadap kerahasiaan, privasi, dan keamanan data mHealth (Atalay & Yücel, 2024). Edukasi singkat mengenai keamanan data dan perlindungan privasi direkomendasikan untuk membantu pengguna mengambil keputusan yang lebih aman. Temuan ini sejalan dengan (Jiang & Zheng, 2023), yang melaporkan bahwa kepercayaan pengguna dalam membagikan data kesehatan dipengaruhi oleh transparansi, pengawasan, dan mekanisme penghapusan data (Meier et al., 2026).

Di Indonesia, perlindungan data pribadi menjadi semakin relevan seiring terus berkembangnya penggunaan layanan digital (Dobson et al., 2023). Oleh karena itu, kegiatan PKM berjudul ‘Sosialisasi Waspada Penyalahgunaan Data Kesehatan Pribadi di Platform Digital/Aplikasi Kesehatan’ diperlukan untuk menumbuhkan perilaku preventif. Kegiatan ini dirancang tidak hanya untuk menyampaikan konsep, tetapi juga melatih peserta untuk memeriksa izin aplikasi, memahami kebijakan privasi, mengaktifkan langkah keamanan akun, dan mengenali situasi yang berpotensi menimbulkan penyalahgunaan data (Flanagan et al., 2025) (Brückner et al., 2025).

Berdasarkan uraian tersebut, tujuan kegiatan ini adalah:

- Meningkatkan pengetahuan peserta mengenai definisi dan jenis data kesehatan pribadi.
- Meningkatkan kesadaran peserta terhadap bentuk penyalahgunaan dan kebocoran data kesehatan di platform digital.
- Melatih peserta memeriksa izin aplikasi, kebijakan privasi, dan pengaturan keamanan akun.
- Meningkatkan kemampuan peserta menerapkan langkah pencegahan sederhana saat menggunakan aplikasi kesehatan.
- Mengukur perubahan pengetahuan peserta melalui pre-test dan post-test.

METODE KEGIATAN

Kegiatan menggunakan metode penyuluhan dan praktik terbimbing. Tahapan kegiatan terdiri atas: (1) identifikasi kebutuhan dan karakteristik peserta; (2) penyusunan materi; (3) pre-test; (4) penyampaian materi; (5) demonstrasi pemeriksaan izin aplikasi dan kebijakan privasi; (6) simulasi kasus; (7) post-test; dan (8) evaluasi serta tindak lanjut.

Sasaran dan Lokasi Kegiatan

Sasaran kegiatan adalah masyarakat/pengguna smartphone yang menggunakan atau berpotensi menggunakan platform digital dan aplikasi kesehatan. Lokasi kegiatan: Puskesmas Ulak Karang Padang. Jumlah peserta: 20 orang. Kegiatan dilaksanakan pada 07 September 2026.

Materi Sosialisasi

Materi sosialisasi disampaikan dalam enam topik utama sebagaimana disajikan pada Tabel 1.

Tabel 1. Materi Sosialisasi Kewaspadaan Penyalahgunaan Data Kesehatan Pribadi

Materi	Topik Utama	Keterampilan yang Dilatih
Data kesehatan pribadi	Identitas, rekam medis, biometrik, obat, diagnosis, lokasi dan data aktivitas	Mengidentifikasi data sensitif
Risiko penyalahgunaan	Kebocoran, akses tanpa izin, phishing, tracking, pihak ketiga	Mengenali skenario risiko
Izin aplikasi	Kamera, lokasi, kontak, mikrofon, penyimpanan	Menilai relevansi permission
Kebijakan privasi	Tujuan pengumpulan, penyimpanan, berbagi dan penghapusan data	Membaca bagian penting privacy policy
Keamanan akun	Password kuat, MFA, pembaruan aplikasi, perangkat aman	Mengaktifkan pengamanan dasar
Respons insiden	Dokumentasi, penggantian kredensial, pelaporan	Menentukan langkah awal ketika terjadi insiden

Evaluasi

Evaluasi pengetahuan dilakukan dengan membandingkan skor pre-test dan post-test. Persentase peningkatan dihitung menggunakan rumus:

Peningkatan (%) = ((Skor post-test – Skor pre-test) / Skor pre-test) × 100%

Apabila diperlukan, perubahan skor dapat dianalisis menggunakan paired t-test untuk data berdistribusi normal atau Wilcoxon signed-rank test untuk data yang tidak memenuhi asumsi normalitas (Andrew et al., n.d.).

HASIL DAN PEMBAHASAN

Hasil

Kegiatan diawali dengan pre-test untuk memetakan pengetahuan awal peserta. Materi kemudian disampaikan melalui presentasi, contoh kasus, dan demonstrasi langsung menggunakan smartphone. Peserta dipandu untuk membuka pengaturan aplikasi, memeriksa izin akses, mengidentifikasi data yang diminta, dan mendiskusikan apakah setiap izin relevan dengan fungsi aplikasi. Pendekatan berbasis demonstrasi dipilih karena isu privasi dapat terasa abstrak apabila hanya dijelaskan secara teoritis.

Materi juga menekankan bahwa persetujuan pengguna tidak boleh dipahami sekadar sebagai tindakan menekan tombol ‘setuju’. Pengguna perlu memahami tujuan pengumpulan data, jenis data yang diproses, pihak yang mungkin menerima data, serta pilihan yang tersedia untuk mengendalikan datanya. Literatur menunjukkan bahwa mekanisme persetujuan yang lebih transparan dapat memperkuat kepercayaan dan kendali pengguna atas data kesehatan (Olsen et al., 2025).

Hasil evaluasi pengetahuan peserta sebelum dan sesudah kegiatan disajikan pada Tabel 2.

Tabel 2. Hasil Evaluasi Pengetahuan Peserta (Pre-test dan Post-test)

Indikator	Pre-test (contoh)	Post-test (contoh)	Peningkatan
Mengenali data kesehatan pribadi	58%	88%	51,7%
Mengenali risiko penyalahgunaan	52%	86%	65,4%
Memeriksa izin aplikasi	45%	84%	86,7%
Memahami kebijakan privasi	40%	78%	95,0%
Mengetahui langkah respons insiden	48%	82%	70,8%

Secara deskriptif, skor pengetahuan peserta meningkat setelah kegiatan sosialisasi. Peningkatan terbesar pada pemahaman kebijakan privasi menunjukkan bahwa materi dan contoh praktis kebijakan privasi dapat membantu peserta mengidentifikasi informasi penting yang sering terlewat. Hasil ini sejalan dengan temuan bahwa pengguna mHealth masih memiliki kesenjangan kesadaran dan memerlukan edukasi mengenai privasi dan keamanan data (Masel et al., 2023).

Pembahasan

Pertama, risiko dapat muncul pada tahap pengumpulan data. Aplikasi dapat meminta akses ke kamera, lokasi, mikrofon, kontak, atau penyimpanan. Permintaan tersebut perlu dibandingkan dengan fungsi aplikasi. Kedua, risiko dapat muncul pada tahap penyimpanan dan transmisi data apabila data tidak dilindungi secara memadai (Sabur et al., n.d.). Ketiga, risiko dapat terjadi ketika data dibagikan kepada pihak ketiga untuk kepentingan analitik, periklanan, penelitian, atau tujuan lain tanpa pemahaman pengguna yang memadai. Studi pemetaan isu etika dan hukum dalam mHealth menunjukkan bahwa pengumpulan dan pertukaran data kesehatan melalui smartphone menciptakan peluang sekaligus risiko privasi yang perlu dikelola (Dobson et al., 2023).

Pengguna juga perlu memahami bahwa keamanan dan privasi merupakan konsep yang saling berkaitan namun tidak identik. Keamanan berfokus pada perlindungan terhadap akses atau penggunaan yang tidak sah, sedangkan privasi berkaitan dengan kendali individu atas bagaimana informasi pribadinya dikumpulkan, digunakan, dan dibagikan (Raab et al., 2023). Sebuah umbrella review terhadap kualitas aplikasi kesehatan menunjukkan bahwa privasi/keamanan data merupakan salah satu kriteria yang sering digunakan untuk menilai aplikasi kesehatan digital (Privatsphäre, 2024) (Farang et al., 2024).

Dari sisi perilaku pengguna, pendekatan edukasi sebaiknya bersifat praktis. Peserta dapat diajarkan prinsip 5T: Teliti memeriksa aplikasi, Tes/tinjau izin aplikasi, Timbang tujuan pengumpulan data, Tingkatkan keamanan akun, dan Tanggap cepat saat terjadi insiden. Prinsip ini dapat menjadi pesan sederhana yang mudah diingat dan diterapkan setelah kegiatan PKM (Flanagan et al., 2025).

Faktor pendukung dan tantangan pelaksanaan kegiatan dirangkum pada Tabel 3.

Tabel 3. Faktor Pendukung dan Tantangan Pelaksanaan Kegiatan

Faktor Pendukung	Tantangan
Antusiasme peserta dan relevansi materi dengan penggunaan smartphone sehari-hari.	Tingkat literasi digital peserta beragam.
Demonstrasi langsung membuat materi lebih mudah dipahami.	Sebagian kebijakan privasi berbahasa teknis dan panjang.
Materi dapat diterapkan pada berbagai aplikasi kesehatan.	Tidak semua peserta menggunakan aplikasi kesehatan secara rutin.

KESIMPULAN

Kegiatan sosialisasi kewaspadaan terhadap penyalahgunaan data kesehatan pribadi merupakan upaya edukasi yang relevan untuk mendukung penggunaan layanan kesehatan digital secara aman. Materi yang menekankan identifikasi data sensitif, pemeriksaan izin aplikasi, pemahaman kebijakan privasi, keamanan akun, dan respons insiden dapat membantu masyarakat mengembangkan perilaku preventif. Evaluasi pre-test

dan post-test perlu digunakan untuk menunjukkan perubahan pengetahuan secara objektif, dan data simulasi pada naskah ini wajib diganti dengan data hasil kegiatan yang sebenarnya sebelum dipublikasikan.

Sebagai tindak lanjut, institusi pendidikan dan fasilitas kesehatan disarankan menyelenggarakan edukasi privasi digital secara berkala, pengembang aplikasi disarankan menyederhanakan kebijakan privasi dan menerapkan prinsip privacy-by-design, pengguna disarankan membatasi izin aplikasi hanya pada yang benar-benar diperlukan, dan kegiatan lanjutan dapat berupa audit sederhana terhadap beberapa aplikasi kesehatan yang umum digunakan oleh peserta.

DAFTAR PUSTAKA

- Andrew, J., Eunice, R. J., & Karthikeyan, J. (n.d.). *An anonymization-based privacy-preserving data collection protocol for digital health data*. 9.
- Atalay, H. N., & Yücel, Ş. (2024). *Decoding privacy concerns : the role of perceived risk and benefits in personal health data disclosure*.
- Brückner, S., Dridi, A., Deshmukh, A., Kirsten, T., Lauber-rönsberg, A., Riedel, R., Hetmank, S., Welzel, C., & Gilbert, S. (2025). *A user-driven consent platform for health data sharing in digital health applications Check for updates*. 1–8.
- Dobson, R., Stowell, M., Warren, J., Tane, T., Ni, L., Gu, Y., Mccool, J., & Whittaker, R. (2023). *Use of Consumer Wearables in Health Research : Issues and Considerations Corresponding Author : 25*, 1–5. <https://doi.org/10.2196/52444>
- Farag, N., Noë, A., Patrinos, D., & Zawati, M. H. (2024). Mapping the Apps : Ethical and Legal Issues with Crowdsourced Smartphone Data using mHealth. In *Asian Bioethics Review*. Springer Nature Singapore. <https://doi.org/10.1007/s41649-024-00296-3>
- Flanagan, L., Poikela, M., & Berlin, U. (2025). *Attitudes of Developers Towards Privacy in Personal Health Applications*. 0. <https://doi.org/10.3233/SHTI250512>
- Jiang, J., & Zheng, Z. (2023). *Personal Information Protection and Privacy Policy Compliance of Health Code Apps in China : Scale Development and Content Analysis*. 11, 1–10. <https://doi.org/10.2196/48714>
- Masel, J., Ian, J., Petrie, M., & Bay, J. (2023). *Combatting SARS-CoV-2 With Digital Contact Tracing and Notification : Navigating Six Points of Failure Corresponding Author : 9*. <https://doi.org/10.2196/49560>
- Meier, M., Maier, C., & Wintm, F. (2026). *Information & Management Privacy over health ? Understanding discontinuous disclosure in mobile health applications*. 63(December 2024). <https://doi.org/10.1016/j.im.2025.104277>
- Nicole, U., Sharief, S., Grace, N., Zepka, E., Mamauag, M., & Clark, L. (2024). Informatics in Medicine Unlocked Access control solutions in electronic health record systems : A systematic review. *Informatics in Medicine Unlocked*, 49(July), 101552. <https://doi.org/10.1016/j.imu.2024.101552>
- Olsen, Q., Dyda, A., Woods, L., Lobo, E., Eden, R., Krahe, M. A., Richards, B., Pather, N., McGee, L., Sullivan, C., & Pole, J. D. (2025). *Worldwide willingness to share health data high but privacy , consent and transparency paramount , a meta-analysis*. 1–13.
- Pool, J., Akhlaghpour, S., Fatehi, F., & Burton-jones, A. (2024). International Journal of Information Management A systematic analysis of failures in protecting personal health data : A scoping review. *International Journal of Information Management*, 74(September 2023), 102719. <https://doi.org/10.1016/j.ijinfomgt.2023.102719>
- Privatsphäre, W. (2024). *Soziale Ungleichheit im Zusammenhang mit digitalen Gesundheitsanwendungen : Digitale Spaltungen in den Bereichen Zugang , Nutzung ,. September 2023*, 268–276. <https://doi.org/10.1007/s00103-024-03832-6>
- Raab, R., Küderle, A., Zakreuskaya, A., Stern, A. D., Klucken, J., Kaissis, G., Rueckert, D., Boll, S., Eils, R., Wagener, H., & Eskofier, B. M. (2023). *Viewpoint Federated electronic health records for the European Health Data Space*. 840–847. [https://doi.org/10.1016/S2589-7500\(23\)00156-5](https://doi.org/10.1016/S2589-7500(23)00156-5)
- Rezaee, R., Khashayar, M., Saeedinezhad, S., & Nasiri, M. (n.d.). *Critical Criteria and Countermeasures for Mobile Health Developers to Ensure Mobile Health Privacy and Security : Mixed Methods Study*

Corresponding Author : 11, 1–13. <https://doi.org/10.2196/39055>

Sabur, A., Arabia, S., Showail, A. J., & Arabia, S. (n.d.). *Nudging Data Privacy of Mobile Health Applications in Saudi Arabia*. 18(1), 1–19. <https://doi.org/10.4018/IJISP.345647>