JURNAL PENGABDIAN
[Vol 4 No 1 Januari 2025] | ISSN 2809-4670 (*Online*)
DOI: https://doi.org/10.36841/mimbarintegritas.v4i1.5571

PENINGKATAN PEMAHAMAN KADER POSYANDU TENTANG KEAMANAN DATA DALAM MENDUKUNG PENGELOLAAN INFORMASI KESEHATAN YANG AMAN

IMPROVING POSYANDU CADRES' UNDERSTANDING OF DATA SECURITY IN SUPPORTING SAFE HEALTH INFORMATION MANAGEMENT

Mohammad Yusuf Setiawan[1)], Diah Wijayanti Sutha[2)*]
[1,2]STIKES Yayasan RS Dr. Soetomo

[2]Email: diahwsutha@gmail.com

Recived: November 28, 2024 *Accepted: December 02, 2024* *Published: December 11, 2024*

Abstrak: Keamanan data kesehatan menjadi salah satu isu penting dalam era digital, terutama pada layanan kesehatan masyarakat seperti posyandu. Kader posyandu memiliki peran strategis dalam pengelolaan informasi kesehatan, namun literasi yang rendah terkait keamanan data dapat meningkatkan risiko kebocoran informasi sensitif. Kegiatan pengabdian masyarakat ini bertujuan untuk meningkatkan pengetahuan dan kesadaran kader posyandu mengenai keamanan data. Metode yang digunakan meliputi sosialisasi interaktif dan pelatihan berbasis studi kasus, yang dilaksanakan di Desa Sukodono. Sebanyak 45 kader posyandu mengikuti kegiatan ini. Evaluasi dilakukan melalui pre-test dan post-test untuk mengukur peningkatan pengetahuan, serta diskusi reflektif untuk menilai potensi implementasi. Hasil menunjukkan peningkatan signifikan pada pemahaman peserta, dengan nilai rata-rata pre-test sebesar 45 meningkat menjadi 85 pada post-test. Peserta juga menunjukkan pemahaman tentang pentingnya menjaga kerahasiaan data dan menerapkan langkah-langkah mitigasi risiko, seperti penggunaan kata sandi yang kuat dan perlindungan data manual. Kegiatan ini berhasil meningkatkan literasi keamanan data kader posyandu, yang diharapkan dapat mendukung pengelolaan informasi kesehatan yang lebih aman dan profesional. Diperlukan upaya lanjutan untuk memperkuat literasi digital kader posyandu guna menghadapi tantangan di era teknologi.

Kata Kunci: Keamanan data, Kader posyandu, Literasi digital

Abstract: *Health data security is an important issue in the digital era, especially in public health services such as integrated health posts. Integrated health post cadres have a strategic role in managing health information, but low literacy regarding data security can increase the risk of sensitive information leakage. This community service activity aims to increase the knowledge and awareness of integrated health post cadres regarding data security. The methods used include interactive socialization and case study-based training, which were carried out in Sukodono Village. A total of 45 integrated health post cadres participated in this activity. Evaluation was carried out through pre-tests and post-tests to measure increased*

knowledge, as well as reflective discussions to assess potential implementation. The results showed a significant increase in participant understanding, with an average pre-test score of 45 increasing to 85 in the post-test. Participants also showed an understanding of the importance of maintaining data confidentiality and implementing risk mitigation measures, such as the use of strong passwords and manual data protection. This activity succeeded in increasing the data security literacy of integrated health post cadres, which is expected to support safer and more professional health information management. Further efforts are needed to strengthen the digital literacy of integrated health post cadres in order to face challenges in the technological era.

Keywords: *Data security, Posyandu cadres, Digital literacy*

PENDAHULUAN

Perkembangan teknologi informasi telah mempermudah akses data yang bermakna. Meskipun teknologi memungkinkan masyarakat umum untuk mengakses data secara akurat dan tepat waktu, namun perhatian terhadap keamanan data masih kurang dalam pengembangan perangkat lunak, yang sering digunakan oleh organisasi yang tidak berkomitmen penuh. Kecepatan pengembangan aplikasi sering kali membahayakan keamanan data, oleh karena itu banyak aplikasi paling populer yang tersedia saat ini memiliki kelemahan yang dapat dimanfaatkan oleh peretas (Cabrera, *et., al.*, 2023; Hussain, *et., al.*, 2020).

Di era digital, data pribadi telah menjadi komoditas yang sangat berharga. Dengan kata lain, semakin banyak data yang diperoleh, semakin besar pula risiko kehilangan data. Masyarakat harus memiliki akses literasi digital yang mudah dipahami agar dapat melindungi diri dari dunia maya yang semakin berbahaya. Literasi digital bukan hanya tentang mengoperasikan perangkat digital, tetapi juga mencakup pemahaman tentang cara bekerja daring, memahami cara mengoperasikan komputer, dan menggunakan prosedur keselamatan yang efektif. Dengan literasi digital, masyarakat dapat memahami berbagai cara beroperasi di dunia maya, menggunakan prosedur keamanan yang tepat, dan memastikan data pribadi tetap aman (Marune, *et., al.*, 2021; Mujtaba, 2024).

Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi dibuat oleh pemerintah. Peraturan ini mendefinisikan data pribadi sebagai data

tentang individu yang dapat diidentifikasi atau dapat diidentifikasi secara terpisah atau dikombinasikan dengan informasi lainnya melalui sistem elektronik atau nonelektronik secara langsung atau tidak langsung. Namun, subjek data pribadi adalah individu yang menyimpan data pribadi. Perlindungan data pribadi bertujuan untuk meningkatkan kesadaran masyarakat tentang pentingnya perlindungan data pribadi dan memastikan bahwa warga negara memiliki hak untuk melindungi diri mereka sendiri.

Hasil laporan survei "Status Literasi Digital di Indonesia", yang dilakukan pada tahun 2022, memberikan gambaran tentang tingkat kesadaran masyarakat tentang keamanan data pribadi. Sebuah survei menilai literasi digital dalam empat pilar: kemampuan digital, moral digital, keamanan digital, dan budaya. Dalam survei tersebut, secara keseluruhan dari pernyataan-pernyataan yang menilai keamanan digital (digital safety), baru separuh dari responden memiliki kebiasaan yang baik untuk melindungi data pribadi; sebagian besar dari mereka telah menunjukkan sikap yang positif tentang masalah ini sendiri, tanpa bantuan orang lain. Hasil penelitian menunjukkan bahwa sebagian masyarakat kurang memahami dan mampu menggunakan sistem perlindungan data pribadi. Peretas dapat mengakses data pribadi karena kerusakan sistem keamanan. Untuk menghindari kebocoran data, masyarakat umum harus mengetahui lebih banyak tentang sistem keamanan digital (KOMINFO, 2023).

Di Dusun Matteko, Desa Erelembang, Kecamatan Tombolo Pao, Kabupaten Gowa, Provinsi Sulawesi Selatan, ada bukti bahwa pelatihan "Langkah-Langkah Bijak di Era Digital: Pelatihan Dasar Keamanan Data Pribadi bagi Masyarakat" telah meningkatkan pemahaman masyarakat Dusun Matteko tentang keamanan data pribadi. Peserta mendapatkan pemahaman yang lebih mendalam tentang ancaman dan metode mudah untuk melindungi data pribadi mereka melalui observasi, materi, dan diskusi. Aktivitas ini tidak hanya memberikan informasi, tetapi juga menciptakan lingkungan kerja sama di mana orang dapat berbagi pengalaman dan lebih memahami satu sama lain (Baso, *et., al.*, 2023).

Puskesmas Sukodono Sidoarjo memiliki visi yang sejalan dengan pelaksanaan pengabdian masyarakat sosialisasi keamanan data pribadi yang merupakan salah satu bentuk dukungan transformasi digital kesehatan, yaitu "Terwujudnya Kabupaten Sidoarjo yang Sejahtera, Maju, Berkarakter dan Berkelanjutan". Berkelanjutan berarti Masyarakat bisa memanfaatkan teknologi digital dengan tetap cermat dalam menjaga data pribadinya. Puskesmas Sukodono telah aktif dalam melakukan kegiatan yang bersifat preventif untuk pencegahan penyakit sehingga kualitas kesehatan warga di wilayah kerja bisa meningkat (Puskesmas Sukodono, 2018). Namun, dari berbagai kegiatan kesehatan yang diselenggarakan oleh Puskesmas Sukodono, belum terlihat adanya kegiatan yang berkaitan dengan peningkatan pengetahuan tentang keamanan data pribadi.

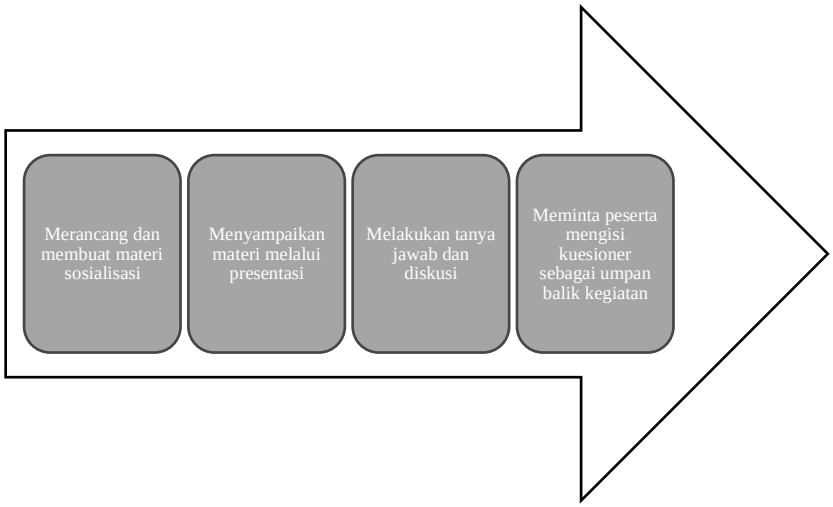
Pada era digital yang semakin terintegrasi ini, hampir seluruh aspek kehidupan yang tidak lepas dari ranah digital. Di samping kemudahan yang ditawarkan, fenomena ini turut menghadirkan tantangan signifikan, terutama dalam hal perlindungan data pribadi. Sebagai bagian dari masyarakat yang terus berkembang, Kader Kesehatan Puskesmas Sukodono juga rentan terhadap kebocoran data pribadi. Masyarakat sering terlibat dalam berbagai aktivitas online, berbagi data melalui internet, dan menyimpan data pribadi di perangkat elektronik. Oleh karena itu, penting bagi setiap anggota masyarakat untuk memahami bahaya dan cara yang dapat dilakukan untuk melindungi data pribadi mereka. Tujuan dari kegiatan ini adalah untuk meningkatkan pengetahuan kader posyandu tentang keamanan data, sehingga mereka dapat membantu membangun sistem pengelolaan informasi kesehatan yang lebih baik.

METODE PELAKSANAAN

Sasaran peserta adalah kader kesehatan dari Puskesmas Sukodono, Kelurahan Jumputrejo, Kecamatan Sukodono, Kabupaten Sidoarjo. Jumlah kader kesehatan sebanyak 60 orang. Namun dari 60 orang tersebut hanya hadir 45 orang. Kegiatan sosialisasi ini dilaksanakan di Kelurahan Jumputrejo, Sukodono, Sidoarjo. Kegiatan ini diikuti oleh 45 peserta dengan rentang usia 26 sampai 61 tahun Seluruh

peserta yang hadir mengikuti seluruh kegiatan acara dari awal acara hingga akhir. Adapun langkah pelaksanaan yang dilakukan dalam kegiatan pengabdian ini adalah sebagai berikut:

1. Merancang dan membuat materi sosialisasi
2. Menyampaikan materi presentasi ke peserta
3. Melakukan tanya jawab dan diskusi
4. Meminta peserta mengisi kuesioner sebagai umpan balik kegiatan



Gambar 1. Tahapan kegiatan pengabdian masyarakat

Kegiatan pengabdian masyarakat ini dilaksanakan di di Kelurahan Jumputrejo, Sukodono, Sidoarjo. Pendekatan yang digunakan adalah metode sosialisasi interaktif dan pelatihan berbasis studi kasus. Pada tahap persiapan dilakukan penyusunan materi sosialisasi yang mencakup pengenalan keamanan data, ancaman terhadap data kesehatan, dan langkah-langkah mitigasi risiko serta pemilihan studi kasus yang relevan dengan kondisi kader posyandu.

Pada pelaksanaan sosialisasi dilakukan dalam bentuk seminar singkat menggunakan media visual dan diskusi kelompok. Pelatihan mencakup simulasi identifikasi potensi kebocoran data serta praktik pengamanan data berbasis teknologi sederhana. Penilaian dilakukan melalui pre-test dan post-test untuk mengukur peningkatan pengetahuan kader. Diskusi reflektif untuk menilai pemahaman dan potensi implementasi materi dalam aktivitas posyandu.

HASIL DAN PEMBAHASAN

Kegiatan ini diikuti oleh 45 kader posyandu dari Kelurahan Jumputrejo, Sukodono, Sidoarjo. Hasil *pre-test* menunjukkan bahwa 70% peserta memiliki pemahaman yang rendah tentang keamanan data, dengan nilai rata-rata 45 dari skala 100. Setelah sosialisasi dan pelatihan, hasil post-test menunjukkan peningkatan signifikan dengan nilai rata-rata 85 dari skala 100. Diskusi kelompok menghasilkan beberapa poin penting, antara lain:

1. Kader memahami pentingnya menjaga kerahasiaan data pasien, terutama data pribadi seperti nomor KTP dan riwayat kesehatan.
2. Kader mulai menyadari risiko penggunaan perangkat teknologi tanpa perlindungan, seperti penggunaan aplikasi pencatat data tanpa enkripsi.
3. Adanya komitmen untuk menerapkan langkah-langkah sederhana seperti penggunaan kata sandi yang kuat dan menjaga kerahasiaan berkas data manual.

Gambar 2. Pemaparan keamanan data oleh narasumber kepada kader posyandu

Hasil ini menunjukkan bahwa pendekatan interaktif yang diterapkan efektif dalam meningkatkan literasi kader mengenai keamanan data. Tantangan yang dihadapi adalah keterbatasan akses teknologi oleh sebagian kader, sehingga perlu adanya dukungan lebih lanjut, seperti pengadaan perangkat pendukung dan pelatihan lanjutan.

JURNAL PENGABDIAN
[Vol 4 No 1 Januari 2025] | ISSN 2809-4670 (*Online*)
DOI: https://doi.org/10.36841/mimbarintegritas.v4i1.5571

Gambar 3. Pelaksanaan *Post-test*

Keamanan data mengacu pada upaya perlindungan informasi dari akses yang tidak sah, kerusakan, atau pencurian. Dalam konteks pelayanan kesehatan, data yang sering dikelola mencakup informasi pribadi seperti identitas pasien, riwayat kesehatan, dan data sensitif lainnya. Kerahasiaan, integritas, dan ketersediaan informasi *(CIA—Confidentiality, Integrity, Availability)* merupakan tiga pilar utama keamanan data yang harus dijaga (Vansuri, *et., al.,* 2023; Yee, *et., al.,* 2021).

Pentingnya keamanan data dalam sektor kesehatan semakin meningkat seiring dengan digitalisasi layanan kesehatan. Kebocoran data pasien dapat menimbulkan dampak serius, seperti pelanggaran privasi, penurunan kepercayaan masyarakat, hingga potensi eksploitasi data untuk tujuan yang merugikan. Contohnya, kasus pelanggaran data kesehatan yang terjadi di Indonesia menunjukkan bahwa lemahnya pengamanan data dapat menimbulkan kerugian besar, baik secara individu maupun institusi (CNBC Indonesia, 2024).

Sebagai pengelola data di tingkat masyarakat, kader posyandu memiliki tanggung jawab besar dalam menjaga keamanan informasi pasien. Namun, keterbatasan literasi digital dan pengetahuan tentang prinsip-prinsip keamanan data sering kali menjadi tantangan. Berdasarkan diskusi dengan kader posyandu dalam kegiatan ini, ditemukan bahwa sebagian besar belum menyadari risiko yang dapat timbul dari pengelolaan data yang tidak aman, seperti: penggunaan alat pencatat manual yang tidak dijaga dengan baik, memungkinkan akses oleh pihak yang tidak

berwenang; ketergantungan pada aplikasi digital tanpa enkripsi, yang dapat mempermudah kebocoran informasi; dan kurangnya pemahaman tentang ancaman siber, seperti *phishing*, *malware*, atau serangan lainnya.

Literasi tentang keamanan data bukan hanya tanggung jawab profesional IT atau petugas kesehatan, tetapi menjadi kebutuhan mendasar bagi semua individu yang mengelola informasi sensitif. Alasan mengapa pemahaman tentang keamanan data menjadi antara lain adalah sebagai perlindungan privasi, di mana Kebocoran data pribadi dapat mengakibatkan penyalahgunaan informasi untuk kejahatan, seperti penipuan atau pencurian identitas. Selanjutnya yaitu mengenai keberlanjutan layanan, dalam konteks posyandu, hilangnya data penting dapat mengganggu layanan kesehatan masyarakat, seperti pelacakan imunisasi atau pemantauan kesehatan ibu dan anak. Kemudian sebagai tanggung jawab hukum dan Undang-undang, seperti UU ITE di Indonesia, mengatur kewajiban perlindungan data pribadi. Pelanggaran hukum dapat berujung pada sanksi pidana dan denda yang signifikan. Terakhir yaitu peningkatan kepercayaan publik, di mana layanan yang menjaga keamanan data pasien akan meningkatkan kepercayaan masyarakat terhadap institusi kesehatan.

Berdasarkan referensi dari National Institute of Standards and Technology (Calder, *et., al.*, 2024; NIST, 2021), berikut adalah langkah-langkah yang dapat diimplementasikan oleh kader posyandu untuk meningkatkan keamanan data:

1. Penyimpanan Aman. Gunakan tempat penyimpanan fisik yang terkunci untuk berkas manual dan perangkat lunak dengan kata sandi yang kuat.
2. Enkripsi Data. Pastikan data yang dikirim atau disimpan dalam format digital dienkripsi untuk mencegah akses tidak sah.
3. Pelatihan Berkala. Berikan pelatihan rutin kepada kader tentang ancaman terbaru dalam keamanan data dan cara mengatasinya.
4. Pengawasan Ketat. Tetapkan aturan yang jelas terkait siapa yang boleh mengakses data dan dalam kondisi apa.
5. Backup Data. Simpan salinan cadangan data penting untuk mencegah kehilangan informasi akibat kerusakan atau bencana.

Dalam kegiatan ini, kader posyandu menunjukkan ketertarikan untuk mempelajari lebih lanjut tentang keamanan data. Melalui diskusi kelompok, muncul beberapa pertanyaan kritis, seperti:

> Bagaimana cara melindungi data manual tanpa teknologi canggih?
> **Jawaban**: Gunakan metode sederhana, seperti buku catatan bersegel, kotak penyimpanan terkunci, dan sistem akses terbatas.
> Apa risiko nyata yang dihadapi kader posyandu dalam konteks lokal?
> **Jawaban**: Misalnya, hilangnya buku register posyandu atau data yang diakses oleh individu yang tidak berkepentingan.

Keamanan data adalah isu universal yang memerlukan perhatian serius dari semua pihak, termasuk kader posyandu. Meningkatkan literasi keamanan data pada kader tidak hanya melindungi data pasien, tetapi juga meningkatkan kualitas pelayanan kesehatan. Dengan memahami ancaman dan menerapkan langkah mitigasi sederhana, kader posyandu dapat berperan lebih aktif dalam menciptakan ekosistem kesehatan yang aman dan terpercaya.

KESIMPULAN

Kegiatan sosialisasi keamanan data kepada kader posyandu telah berhasil meningkatkan pemahaman mereka tentang pentingnya menjaga kerahasiaan informasi kesehatan. Kader posyandu kini memiliki pengetahuan dasar tentang ancaman terhadap data kesehatan dan langkah-langkah pengamanan yang dapat diterapkan. Kegiatan ini memberikan manfaat langsung bagi pengelolaan data kesehatan di tingkat posyandu sekaligus menjadi model pengembangan literasi digital di masyarakat. Ke depan, diperlukan program berkelanjutan untuk memperkuat kapasitas kader dalam memanfaatkan teknologi secara aman.

UCAPAN TERIMA KASIH

Kami mengucapkan terima kasih yang sebesar-besarnya kepada Pemerintah Desa Sukodono dan seluruh kader kesehatan dari Puskesmas Sukodono, Kelurahan Jumputrejo, Kecamatan Sukodono, Kabupaten Sidoarjo yang telah berpartisipasi aktif dalam kegiatan pengabdian masyarakat ini. Apresiasi juga kami sampaikan

kepada STIKES Yayasan RS Dr. Soetomo atas dukungan fasilitas dan koordinasi yang telah diberikan, sehingga kegiatan ini dapat berjalan dengan lancar. Penghargaan khusus kami berikan kepada tim pengabdian masyarakat yang telah bekerja keras dalam perencanaan, pelaksanaan, dan evaluasi program ini. Terima kasih juga kepada seluruh pihak yang tidak dapat kami sebutkan satu per satu atas kontribusi dan dukungannya. Semoga kegiatan ini dapat memberikan manfaat yang berkelanjutan bagi kader posyandu dan masyarakat, serta menjadi langkah awal dalam pengembangan literasi digital dan pengelolaan informasi kesehatan yang aman di tingkat lokal.

DAFTAR PUSTAKA

Baso, Fadhlirrahman, Isma, A., Fadhilah, N., & Surianto, D. F. (2023). Langkah-Langkah Bijak di Era Digital: Pelatihan Dasar Keamanan Data Pribadi bagi Masyarakat. *Jurnal Kemitraan Responsif Untuk Aksi Inovatif Dan Pengabdian Masyarakat*, 73–79.

Cabrera, Mantilla, C. E., Barba-Vera, R., Rivera, L. M. N., & Pumagualli, M. L. V. (2023). Data Base Security Technologies That Healp Protect Against Misuse By External Hackers Related Reseach Article. *Russian Law Journal*, *11*(9), 334–344. https://cyberleninka.ru/article/n/data-base-security-technologies-that-help-protect-against-misuse-by-external-hackers-related-research-articles

Calder, Alan, & Watkins, S. (2024). *IT governance: an international guide to data security and ISO 27001/ISO 27002*.

CNBC Indonesia. (2024). *1,4 Juta Data Kesehatan Bocor, Terbesar Sepanjang 2024*. CNBC. https://www.cnbcindonesia.com/tech/20240805150532-37-560496/14-juta-data-kesehatan-bocor-terbesar-sepanjang-2024

Hussain, S. A., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. *MDPI*, *8*(2), 133. https://doi.org/https://doi.org/10.3390/healthcare8020133

KOMINFO. (2023). *Status Literasi Digital di Indonesia*.

Marune, Sahat, A. E. M., & Hartanto, B. (2021). Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective. *International Journal of Business, Economics, and Social Development*, *2*(4), 143–152. https://journal.rescollacomm.com/index.php/ijbesd/article/view/170

Mujtaba, B. G. (2024). Cybercrimes and safety policies to protect data and organizations. *Journal of Crime and Criminal Behavior*, *4*(1), 91–112. https://www.arfjournals.com/image/catalog/Journals Papers/JCCB/2024/No 1 (2024)/4_Bahaudin.pdf

NIST. (2021). *Data Security*. NIST. https://www.nccoe.nist.gov/data-security

Presiden RI. (2022). *Undang-undang Perlindungan Data Pribadi*. *016999*, 1–50.

Puskesmas Sukodono. (2018). *Visi dan Misi Puskesmas Sukodono*.

Vansuri, Rayhan, Fauzi, A., Prasetyo, E. T., Negara, R., Ramadhan, R., Restu, A. M., & Raffi, R. F. (2023). Peran CIA (Confidentiality, Integrity, Availability) Terhadap Manajemen Keamanan Informasi. *Jurnal Ilmu Multidisiplin*, *2*(1), 106–113.

Yee, Kar, C., & Zolkipli, M. F. (2021). Review on confidentiality, integrity and availability in information security. *Journal of ICT in Education*, *8*(2), 34–42.