Jurnal Pengabdian Masyarakat Variasi
ISSN: 3048-1406 (Online - Elektronik)
Vol. 3, No. 1, Januari 2026 Hal. 7-12
https://ejurnal.stmikmethodistbinjai.ac.id/jpmv

Edukasi dan Pendampingan Keamanan Data Pasien dalam Menghadapi Risiko Kebocoran Data pada Layanan Fintech di Lingkungan uskesmas

Ayumi Kartika Sari [1*] , Raja Nasrul Fuad[2]

[1]Ilmu Hukum, Fakultas Hukum, Universitas Prima Indonesia, Indonesia
Jl. Sampul No. 3, Kelurahan Sei Putih Barat, Medan, Sumatera Utara, Indonesia
[2]Teknologi Informasi, Fakultas Teknik dan Ilmu Komputer, Universitas Deli Sumatera
Jalan Jenderal Besar Abdul Haris Nasution No. 11 CDE, Medan, Sumatera Utara, Indonesia
Email: [1*]ayumikartikasari@unprimdn.ac.id
(*: coressponding author)

Abstrak

Transformasi digital dalam layanan kesehatan mendorong pemanfaatan platform financial technology (fintech) sebagai sistem pembayaran di Puskesmas. Namun, penggunaan layanan fintech berpotensi menimbulkan risiko kebocoran data pribadi pasien apabila tidak didukung oleh pemahaman hukum dan penerapan keamanan sistem informasi yang memadai. Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan literasi hukum perlindungan konsumen serta kapasitas teknis tenaga kesehatan dalam menjaga keamanan data pasien di Puskesmas Hamparan Perak. Metode pelaksanaan meliputi sosialisasi regulasi perlindungan data pribadi, pelatihan dasar keamanan sistem informasi (password management, autentikasi dua faktor, enkripsi data), serta pendampingan identifikasi risiko kebocoran data pada proses transaksi fintech. Kegiatan dilakukan melalui pendekatan edukatif-partisipatif dengan sesi diskusi, simulasi kasus, dan evaluasi pemahaman peserta. Hasil kegiatan menunjukkan peningkatan pemahaman tenaga kesehatan mengenai prinsip perlindungan data pribadi dan langkah mitigasi risiko kebocoran data pada layanan fintech. Selain itu, tersusun rekomendasi prosedur sederhana pengamanan data pasien yang dapat diterapkan secara berkelanjutan. Program ini diharapkan mampu memperkuat kesadaran hukum dan keamanan digital di lingkungan Puskesmas, sehingga perlindungan data pasien sebagai bagian dari hak konsumen layanan kesehatan dapat terjamin secara lebih optimal di era transformasi digital.

Kata Kunci: Perlindungan Data Pribadi; Keamanan Sistem Informasi; Fintech Kesehatan; Perlindungan Konsumen; Puskesmas Hamparan Perak.

Abstract

Digital transformation in healthcare services has encouraged the utilization of financial technology (fintech) platforms as payment systems in Public Health Centers (Puskesmas). However, the use of fintech services may pose risks of personal data breaches if not supported by adequate legal understanding and proper implementation of information system security. This community service activity aims to enhance legal literacy on consumer protection and improve the technical capacity of healthcare personnel in safeguarding patient data at Hamparan Perak Public Health Center. The implementation methods included the dissemination of personal data protection regulations, basic training on information system security (password management, two-factor authentication, and data encryption), and assistance in identifying potential data breach risks in fintech transaction processes. The program was conducted using an educational-participatory approach through discussion sessions, case simulations, and participant comprehension evaluations. The results indicate an improvement in healthcare personnel's understanding of personal data protection principles and mitigation strategies against data breach risks in fintech services. In addition, a set of simple and sustainable procedural recommendations for securing patient data was developed. This program is expected to strengthen legal awareness and digital security practices within the Public Health Center environment, ensuring that patient data protection as part of consumer rights in healthcare services can be more effectively guaranteed in the era of digital transformation.

Keywords: Personal Data Protection; Information System Security; Health Fintech; Consumer Protection; Hamparan Perak Public Health Center.

1. PENDAHULUAN

Transformasi digital telah mendorong perubahan signifikan dalam tata kelola layanan kesehatan, termasuk pada fasilitas pelayanan tingkat pertama seperti Puskesmas. Pemanfaatan sistem informasi kesehatan dan integrasi layanan pembayaran berbasis digital, termasuk financial technology (fintech), menjadi bagian dari upaya meningkatkan efisiensi, transparansi, dan kualitas pelayanan publik. Digitalisasi transaksi keuangan di sektor kesehatan memberikan kemudahan bagi pasien dalam melakukan pembayaran serta mempercepat proses administrasi. Namun, di balik kemudahan tersebut, muncul tantangan baru terkait keamanan dan perlindungan data pribadi pasien yang tersimpan dan diproses secara elektronik (Kartika Sari et al., n.d.)

Data pasien, termasuk identitas, riwayat kesehatan, dan informasi finansial, tergolong sebagai data pribadi yang bersifat sensitif. Dalam konteks hukum di Indonesia, perlindungan terhadap data pribadi telah diatur melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang menegaskan kewajiban pengendali dan pemroses data untuk menjamin keamanan serta kerahasiaan informasi pribadi. Selain itu, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen juga memberikan landasan bahwa setiap konsumen berhak atas kenyamanan, keamanan, dan keselamatan dalam menggunakan barang dan/atau jasa. Dengan demikian, pasien sebagai konsumen layanan kesehatan berhak memperoleh jaminan perlindungan atas data pribadinya dalam setiap transaksi, termasuk transaksi berbasis fintech (Kartika Sari et al., n.d.).

Di sisi lain, perkembangan fintech di Indonesia menunjukkan pertumbuhan yang pesat dan semakin terintegrasi dalam berbagai sektor, termasuk kesehatan. Otoritas Jasa Keuangan (OJK) menegaskan bahwa penyelenggara fintech wajib menerapkan prinsip manajemen risiko, keamanan sistem informasi, serta perlindungan data konsumen dalam operasionalnya (OJK, 2023). Meskipun demikian, berbagai kasus kebocoran data dan serangan siber di Indonesia menunjukkan bahwa ancaman terhadap keamanan informasi masih menjadi persoalan serius. Lemahnya literasi keamanan digital dan belum optimalnya penerapan standar keamanan sistem informasi pada tingkat operasional dapat meningkatkan risiko terjadinya data breach, baik akibat kesalahan manusia (human error) maupun serangan eksternal.

Berdasarkan kondisi tersebut, diperlukan upaya preventif melalui edukasi dan pendampingan kepada tenaga kesehatan dan pengelola administrasi di Puskesmas agar memiliki pemahaman yang komprehensif mengenai aspek hukum dan teknis perlindungan data pribadi. Pendekatan yang mengintegrasikan perspektif hukum perlindungan konsumen dengan praktik keamanan sistem informasi menjadi penting untuk membangun budaya keamanan digital (digital security awareness) di lingkungan layanan kesehatan. Dengan peningkatan kapasitas sumber daya manusia, diharapkan risiko kebocoran data pasien dalam penggunaan layanan fintech dapat diminimalisir, sekaligus memperkuat akuntabilitas dan kepercayaan masyarakat terhadap pelayanan kesehatan berbasis digital.(Yuttama et al., 2022)(Putri Damayanti, 2024)

2. TINJAUAN PUSTAKA

2.1 Perlindungan Data Pribadi dalam Perspektif Hukum

Perlindungan data pribadi merupakan bagian dari hak privasi yang diakui sebagai hak fundamental warga negara dalam era digital. Di Indonesia, pengaturan mengenai perlindungan data pribadi secara komprehensif diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Undang-undang ini menegaskan kewajiban pengendali data untuk memproses data pribadi secara sah, terbatas, dan transparan, serta memastikan keamanan data melalui langkah teknis dan organisasi yang memadai. Data kesehatan dikategorikan sebagai data pribadi yang bersifat spesifik dan sensitif, sehingga membutuhkan tingkat perlindungan yang lebih tinggi dibandingkan data umum (UU No. 27 Tahun 2022).

Selain itu, dalam perspektif perlindungan konsumen, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen menyatakan bahwa konsumen berhak atas kenyamanan, keamanan, dan keselamatan dalam menggunakan barang dan/atau jasa. Dalam konteks layanan kesehatan berbasis digital, pasien merupakan konsumen jasa kesehatan yang berhak atas perlindungan atas data pribadinya. Dengan demikian, kebocoran data pasien dapat dikategorikan sebagai bentuk pelanggaran terhadap hak konsumen apabila terjadi akibat kelalaian penyelenggara layanan (UU No. 8 Tahun 1999).

2.2 Financial Technology (Fintech) dan Risiko Keamanan Data

Financial Technology (fintech) merupakan inovasi layanan keuangan berbasis teknologi informasi yang memanfaatkan sistem elektronik dan jaringan internet untuk meningkatkan efisiensi transaksi keuangan. Di Indonesia, penyelenggaraan fintech diawasi oleh Otoritas Jasa Keuangan (OJK) yang mewajibkan penerapan manajemen risiko dan perlindungan konsumen dalam setiap operasionalnya (OJK, 2023). Pemanfaatan fintech dalam sektor kesehatan, khususnya sebagai sistem pembayaran di fasilitas layanan kesehatan, memberikan kemudahan dan transparansi dalam pengelolaan transaksi.(Kusuma Dewi & Mardiana, 2023)(Harsuti et al., 2023)

Namun, digitalisasi transaksi juga meningkatkan potensi risiko keamanan informasi, seperti serangan siber, pencurian identitas, phishing, dan kebocoran data akibat lemahnya pengamanan sistem. Menurut ISACA (2019), tata kelola teknologi informasi yang efektif harus mencakup pengendalian keamanan, manajemen risiko, serta pemantauan berkelanjutan terhadap sistem informasi. Tanpa penerapan standar

keamanan yang memadai, penggunaan fintech dapat membuka celah kerentanan yang berdampak pada hilangnya kepercayaan public (Sari et al., 2025)

2.3 Keamanan Sistem Informasi dan Mitigasi Kebocoran Data

Keamanan sistem informasi merupakan serangkaian kebijakan, prosedur, dan teknologi yang dirancang untuk melindungi kerahasiaan (confidentiality)(Tania et al., 2024), integritas (integrity)(Nasution et al., 2026), dan ketersediaan (availability) data. Prinsip CIA Triad menjadi dasar dalam pengelolaan keamanan informasi modern (Whitman & Mattord, 2021). Dalam konteks layanan kesehatan, pengamanan data pasien memerlukan penerapan kontrol teknis seperti enkripsi data, autentikasi dua faktor, manajemen akses berbasis peran (role-based access control), serta pembaruan sistem secara berkala.(Ayumi Kartika Sari, 2025)

Selain aspek teknis, faktor sumber daya manusia juga berperan penting dalam mencegah kebocoran data. Human error sering kali menjadi penyebab utama insiden keamanan informasi. Oleh karena itu, peningkatan literasi keamanan digital dan pelatihan berkelanjutan bagi tenaga kesehatan menjadi strategi preventif yang efektif. Pendekatan edukatif-partisipatif dalam kegiatan pengabdian masyarakat dapat memperkuat kesadaran hukum sekaligus meningkatkan kompetensi teknis dalam menjaga keamanan data pasien di lingkungan Puskesmas.(Muhammad Syahputra Novelan, 2024)(Dani et al., 2024)

3. METODE PELAKSANAAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan desain partisipatif yang dipadukan dengan metode evaluasi pre-test dan post-test untuk mengukur peningkatan pemahaman peserta. Pendekatan ini dipilih karena penelitian berfokus pada analisis pemahaman hukum dan kesiapan teknis tenaga kesehatan dalam menghadapi risiko kebocoran data pada penggunaan layanan fintech di Puskesmas Hamparan Perak. Model kegiatan dilaksanakan dalam bentuk edukasi, pelatihan, dan pendampingan teknis yang terintegrasi antara aspek hukum perlindungan konsumen dan aspek keamanan sistem informasi (Munzir et al., 2023).

3.1 Lokasi dan Subjek Penelitian

Penelitian dilaksanakan di Puskesmas Hamparan Perak. Subjek penelitian terdiri dari tenaga kesehatan, staf administrasi, serta petugas yang terlibat dalam pengelolaan sistem pembayaran berbasis fintech. Pemilihan subjek dilakukan secara purposive sampling, yaitu peserta yang secara langsung berinteraksi dengan data pasien dan sistem transaksi digital.

3.2 Lokasi dan Subjek Penelitian

Teknik pengumpulan data dilakukan melalui:

1. Observasi langsung, untuk mengidentifikasi alur transaksi fintech dan potensi risiko kebocoran data.
2. Wawancara semi-terstruktur, guna menggali pemahaman peserta mengenai perlindungan data pribadi dan keamanan sistem informasi.
3. Kuesioner pre-test dan post-test, untuk mengukur peningkatan literasi hukum dan pemahaman teknis keamanan digital.
4. Dokumentasi, berupa catatan kegiatan, materi pelatihan, serta evaluasi hasil pendampingan.

3.3 Tahapan Pelaksanaan

Tahapan Penelitian Meliputi :

1. Identifikasi Masalah : Analisis awal terhadap praktik penggunaan fintech dan pengelolaan data pasien.
2. Perancangan Materi Edukasi : Penyusunan materi terkait regulasi perlindungan data pribadi, hak konsumen, serta dasar keamanan sistem informasi.
3. Pelaksanaan Sosialisasi dan Pelatihan : Penyampaian materi hukum dan praktik teknis seperti password management, autentikasi dua faktor, dan enkripsi data.
4. Pendampingan dan Simulasi Kasus : Identifikasi risiko dan penyusunan rekomendasi prosedur pengamanan data.
5. Evaluasi dan Analisis : Perbandingan hasil pre-test dan post-test serta analisis kualitatif terhadap peningkatan pemahaman peserta.

Jurnal Pengabdian Masyarakat Variasi
ISSN: 3048-1406 (Online - Elektronik)
Vol. 3, No. 1, Januari 2026 Hal. 7-12
https://ejurnal.stmikmethodistbinjai.ac.id/jpmv

3.4 Teknik Analisis Data

Data kualitatif dianalisis menggunakan teknik reduksi data, penyajian data, dan penarikan kesimpulan. Sementara itu, data kuantitatif dari hasil pre-test dan post-test dianalisis secara deskriptif untuk melihat persentase peningkatan pemahaman peserta.

Melalui metode ini, penelitian diharapkan mampu memberikan gambaran komprehensif mengenai efektivitas edukasi dan pendampingan dalam meningkatkan perlindungan data pasien serta meminimalkan risiko kebocoran data pada penggunaan layanan fintech di Puskesmas.

4. HASIL DAN PELAKSANAAN

Kegiatan pengabdian kepada masyarakat ini dilaksanakan di Puskesmas Hamparan Perak dengan melibatkan tenaga kesehatan dan staf administrasi yang berperan dalam pengelolaan data pasien serta transaksi pembayaran berbasis fintech. Pelaksanaan kegiatan difokuskan pada peningkatan literasi hukum perlindungan data pribadi dan penguatan kapasitas teknis keamanan sistem informasi guna meminimalkan risiko kebocoran data. Bagian ini menyajikan hasil pelaksanaan kegiatan yang meliputi proses sosialisasi, pelatihan teknis, pendampingan identifikasi risiko, serta evaluasi peningkatan pemahaman peserta terhadap aspek perlindungan konsumen dan keamanan digital di lingkungan Puskesmas..

4.1 Hasil Pelaksanaan Sesi Materi dan Praktik

Pelaksanaan sesi materi diawali dengan pemaparan mengenai urgensi perlindungan data pribadi dalam layanan kesehatan, khususnya pada penggunaan sistem pembayaran berbasis fintech di Puskesmas. Materi hukum menekankan kewajiban institusi dalam melindungi data pasien berdasarkan Undang-Undang Perlindungan Data Pribadi serta prinsip perlindungan konsumen dalam transaksi digital. Peserta diberikan pemahaman mengenai kategori data sensitif, potensi risiko kebocoran data, serta konsekuensi hukum dan administratif apabila terjadi pelanggaran keamanan informasi. Diskusi interaktif dilakukan untuk menggali pemahaman awal peserta terkait praktik pengelolaan data yang selama ini diterapkan.

Selanjutnya, sesi praktik difokuskan pada penguatan kapasitas teknis keamanan sistem informasi. Peserta dilatih mengenai penerapan password management yang kuat, penggunaan autentikasi dua faktor (two-factor authentication), pengelolaan akses berbasis peran (role-based access control), serta pentingnya enkripsi data dalam transaksi digital. Selain itu, dilakukan simulasi kasus kebocoran data dan serangan phishing untuk meningkatkan kewaspadaan terhadap ancaman siber. Hasil evaluasi melalui pre-test dan post-test menunjukkan adanya peningkatan pemahaman peserta terhadap prinsip perlindungan data pribadi dan langkah mitigasi risiko kebocoran data. Secara umum, peserta menunjukkan peningkatan kesadaran akan pentingnya menjaga kerahasiaan data pasien sebagai bagian dari tanggung jawab profesional dan perlindungan hak konsumen layanan kesehatan.

Gambar 4.1 Pelaksanaan Sesi Materi dan Praktik Keamanan Data di Puskesmas Hamparan Perak

Jurnal Pengabdian Masyarakat Variasi
ISSN: 3048-1406 (Online - Elektronik)
Vol. 3, No. 1, Januari 2026 Hal. 7-12
https://ejurnal.stmikmethodistbinjai.ac.id/jpmv

4.2 Dokumentasi Kegiatan dan Tindak Lanjut

Dokumentasi kegiatan dilakukan secara sistematis melalui pencatatan daftar hadir peserta, pengambilan dokumentasi foto selama sesi sosialisasi dan praktik, serta pengumpulan hasil evaluasi tertulis. Dokumentasi ini menjadi bagian dari laporan kegiatan sekaligus bukti pelaksanaan program pengabdian kepada masyarakat. Selain itu, materi pelatihan dan panduan teknis keamanan data dibagikan dalam bentuk softcopy kepada pihak Puskesmas agar dapat digunakan sebagai referensi internal secara berkelanjutan.

Sebagai tindak lanjut, disusun rekomendasi prosedur operasional standar (SOP) sederhana terkait pengamanan data pasien dalam transaksi fintech, meliputi pembaruan kata sandi secara berkala, pembatasan hak akses sistem, pencatatan aktivitas login, serta edukasi rutin mengenai keamanan digital. Pihak Puskesmas juga didorong untuk melakukan evaluasi berkala terhadap sistem pembayaran digital yang digunakan serta meningkatkan koordinasi dengan penyedia layanan fintech terkait standar keamanan data. Dengan adanya tindak lanjut ini, diharapkan keberlanjutan program dapat terjaga dan budaya keamanan informasi di lingkungan Puskesmas semakin kuat, sehingga risiko kebocoran data pasien dapat diminimalkan secara optimal.

Gambar 4.2 Foto Bersama Pasien Di Puskesmas Hamparan Perak

Gambar 2 memperlihatkan dokumentasi kegiatan pengabdian kepada masyarakat yang dilaksanakan di Puskesmas Hamparan Perak, meliputi sesi diskusi akhir, pengisian daftar hadir, serta foto bersama antara tim pelaksana dan peserta. Pada tahap ini juga dilakukan penyampaian rekomendasi tindak lanjut berupa penyusunan prosedur operasional standar (SOP) pengamanan data pasien dalam transaksi fintech, pembaruan kata sandi secara berkala, dan peningkatan pengawasan akses sistem. Dokumentasi ini menjadi bukti pelaksanaan kegiatan sekaligus dasar evaluasi untuk memastikan keberlanjutan program dalam memperkuat budaya keamanan informasi di lingkungan Puskesmas.

5. KESIMPULAN

Kegiatan pengabdian kepada masyarakat yang dilaksanakan di Puskesmas Hamparan Perak menunjukkan bahwa integrasi edukasi hukum perlindungan data pribadi dan pelatihan keamanan sistem informasi memiliki peran penting dalam meningkatkan kesiapan tenaga kesehatan menghadapi risiko kebocoran data pada penggunaan layanan fintech. Transformasi digital di sektor kesehatan tidak hanya menuntut efisiensi layanan, tetapi juga tanggung jawab institusi dalam menjaga kerahasiaan dan keamanan data pasien sebagai bagian dari hak konsumen layanan kesehatan. Hasil pelaksanaan kegiatan menunjukkan adanya peningkatan pemahaman peserta terhadap regulasi perlindungan data pribadi, prinsip perlindungan konsumen, serta langkah-langkah teknis mitigasi risiko seperti pengelolaan kata sandi yang aman, autentikasi dua faktor, dan pembatasan akses sistem. Selain peningkatan aspek kognitif, kegiatan ini juga mendorong terbentuknya kesadaran kolektif mengenai pentingnya budaya keamanan digital di lingkungan Puskesmas. Dengan adanya rekomendasi prosedur pengamanan data dan komitmen tindak lanjut dari pihak Puskesmas, diharapkan praktik perlindungan data pasien dapat diterapkan secara berkelanjutan. Program ini menjadi langkah strategis dalam memperkuat tata kelola keamanan informasi pada layanan kesehatan berbasis digital, sehingga kepercayaan masyarakat terhadap sistem pembayaran fintech dan layanan kesehatan dapat terjaga secara optimal di era transformasi digital.

Daftar Pustaka

Ayumi Kartika Sari. (2025). Kebijakan Hukum Perlindungan Konsumen terhadap Kebocoran Data di Platform Fintech. *Judge : Jurnal Hukum*, *6*(2).

Dani, R., Marsyaf, A., Wiarta, I., & Hierdawati, T. (2024). Pelatihan Pengenalan Financial Technology (Fintech) Bagi Mahasiswa Peserta Program Pembinaan Mahasiswa Wirausaha (P2MW) Kemendikbudristek. *Dinamika Sosial : Jurnal Pengabdian Masyarakat Dan Transformasi Kesejahteraan*, *1*(2), 65–74. https://doi.org/10.62951/dinsos.v1i2.231

Harsuti, H., Safitri Pantja Koesoemasari, D., Pahlevi, A., & Kusuma Wardana, R. (2023). Kuras Institute Scidac Plus Artikel ini menggunakan lisensi Creative Commons Attribution 4.0 International License Pengenalan Financial Technology Pada Pelaku UMKM. In *Jurnal Pengabdian Multidisiplin* (Vol. 3).

Kartika Sari, A., Nasrul Fuad, R., & Muhammad Syahputra Novelan, dan. (n.d.). *Sosialisasi Perlindungan Hukum Transaksi Digital dan Penerapan Fintech untuk Pembayaran Layanan Kesehatan di Puskesmas Hamparan Perak*.

Kusuma Dewi, I., & Mardiana, S. (2023). Financial Technology (Fintech) sebagai Faktor Pendorong Peningkatan UMKM di Ciseeng-Bogor. In *Praxis: Jurnal Pengabdian Kepada Masyarakat* (Vol. 3, Number 1). http://pijarpemikiran.com/

Muhammad Syahputra Novelan. (2024). Pelatihan Pemanfaatan Teknologi Informasi untuk Meningkatkan Kesadaran Hukum di Masyarakat Desa Kelambir V Kebun Kecamatan Hamparan Perak. *JURNAL HASIL PENGABDIAN MASYARAKAT (JURIBMAS)*, *3*(1), 8–13.

Munzir, M., Danuwijaya, T., Tunang, A., Dinar, L., & Kassa, P. (2023). Edukasi Financial Technology (FINTECH) pada Pelajar di Kota Sorong. *Samakta: Jurnal Pengabdian Kepada Masyarakat*, *1*(1), 28–35. https://doi.org/10.61142/samakta.v1i1.59

Nasution, A. Y., Alasi, T. S., Manalu, P. D., Irawan, D., & Rosnelly, R. (2026). *Keamanan Data Dengan Analisis Log Berbasis Kecerdasan Buatan* (I. Taufik, Ed.; pp. 1–105). Media Publiaksi Idpress. https://www.media-publikasi-idpress.my.id/2026/01/15.html

Putri Damayanti, A. M. S. R. A. A. (2024). ASPEK HUKUM PENGGUNAAN FINTECH DALAM INDUSTRI PERBANKAN: GUNA MENINGKATKAN KEAMANAN, INOVASI, DAN PERLINDUNGAN KONSUMEN. *Jurnal Ilmiah Penelitian Mahasiswa*, *02*(06).

Sari, A. K., Syahputra Novelan, M., & Nababan, A. A. (2025). *Pelatihan Penerapan Sistem Informasi Berbasis Komputer Untuk Pengelolaan Arsip Hukum Pada Kantor Desa* (Vol. 02, Number 01).

Tania, M., Alasi, T. S., & Yap, R. (2024). ALGORITMA AES UNTUK KEAMANAN DATA DIGITAL BERBASIS WEB DI KANTOR DESA AMAN DAMAI. *Jurnal TIMES*, *13*(2), 142–149.

Yuttama, F. R., Alfizi, A., & Widadi, B. (2022). Pelatihan Financial Technology untuk Bertransaksi dan Berinvestasi. *Jurnal Pengabdian Masyarakat - PIMAS*, *1*(3), 147–152. https://doi.org/10.35960/pimas.v1i3.816