Indonesian Journal of Health Science
Volume 6 No.3, 2026

DATA SECURITY AND PUBLIC TRUST IN THE DIGITALIZATION OF HEALTH INSURANCE IN INDONESIA: A LITERATURE REVIEW

LITERATUR REVIEW: KEAMANAN DATA DAN KEPERCAYAAN PUBLIK DALAM DIGITALISASI ASURANSI KESEHATAN DI INDONESIA

Amanda Safitri [1]; Siti Aisyah [2]; Nadia Putri Untiami [3]; Cahya Arbitera [4]; Riswandy Wasir [5]

[1] amandasafitrii128@gmail.com, *Universitas Pembangunan Nasional "Veteran" Jakarta*
[2] sitiaisyahh954@gmail.com, *Universitas Pembangunan Nasional "Veteran" Jakarta*
[3] nadiauntiami@gmail.com,*Universitas Pembangunan Nasional "Veteran" Jakarta*
[4] cahyaarbitera@upnvj.ac.id, *Universitas Pembangunan Nasional "Veteran" Jakarta*
[5] riswandywasir@upnvj.ac.id, *Universitas Pembangunan Nasional "Veteran" Jakarta*

Abstract
The digitalization of health insurance in Indonesia, particularly in the implementation of the National Health Insurance (JKN) program, offers significant benefits in improving the efficiency and accessibility of healthcare services. However, this digital transformation also presents serious challenges related to data security and public trust. This study aims to examine the relationship between data security and public trust in the context of health insurance digitalization through a literature review approach. The method used is descriptive-analytical by reviewing relevant scientific articles published between 2020 and 2026, obtained from databases such as Google Scholar, Garuda, and other international sources. The findings indicate that data security risks, including data breaches, cybercrime, and weak data governance, are key factors that may reduce public trust in digital health insurance services. In addition, non-technical factors such as low privacy literacy and human error further increase system vulnerabilities. On the other hand, public trust is influenced not only by technical security but also by perceived benefits, transparency, and ethical governance. Therefore, strengthening data security systems, adopting innovative technologies, and developing trust-based governance are essential to support the sustainability of health insurance digitalization in Indonesia.
Keywords*: Cybersecurity; Data Governance; Data Security; Digitalization; Privacy; Public Trust*

Abstrak
Digitalisasi asuransi kesehatan di Indonesia, khususnya dalam pelaksanaan Program Jaminan Kesehatan Nasional (JKN), membawa berbagai manfaat dalam meningkatkan efisiensi dan akses layanan kesehatan. Namun, transformasi digital tersebut juga menimbulkan tantangan serius terkait keamanan data dan kepercayaan publik. Penelitian ini bertujuan untuk mengkaji hubungan antara keamanan data dan kepercayaan publik dalam konteks digitalisasi asuransi kesehatan melalui pendekatan studi literatur. Metode yang digunakan adalah deskriptif-analitis dengan menelaah berbagai artikel ilmiah yang relevan dari tahun 2020–2026 yang diperoleh melalui basis data seperti Google Scholar, Garuda, dan database internasional lainnya. Hasil kajian menunjukkan bahwa risiko keamanan data, seperti kebocoran informasi, kejahatan siber, dan kelemahan tata kelola data, menjadi faktor utama yang dapat menurunkan kepercayaan masyarakat terhadap layanan asuransi digital. Selain itu, faktor non-teknis seperti rendahnya literasi privasi dan human error turut memperburuk kerentanan sistem. Di sisi lain, kepercayaan publik dipengaruhi tidak hanya oleh keamanan teknis, tetapi juga oleh manfaat yang dirasakan, transparansi, serta tata kelola berbasis etika. Oleh karena itu, diperlukan penguatan sistem keamanan data, penerapan teknologi inovatif, serta pengembangan tata kelola berbasis kepercayaan untuk mendukung keberlanjutan digitalisasi asuransi kesehatan di Indonesia.
Kata Kunci: Digitalisasi; Keamanan Data; Kepercayaan Publik; Privasi; Siber; Tata Kelola Data

PENDAHULUAN

Kesehatan merupakan pilar esensial dalam agenda pembangunan nasional, sebuah prinsip yang selaras dengan kerangka Tujuan Pembangunan Berkelanjutan (SDGs) yang dirancang oleh Perserikatan Bangsa-Bangsa. Sebagai negara berkembang dengan demografi terbesar keempat di dunia, Indonesia menghadapi hambatan struktural dalam menjamin pemerataan dan kualitas akses layanan kesehatan bagi seluruh masyarakat. Merespon tantangan

tersebut, pemerintah telah mengimplementasikan Program Jaminan Kesehatan Nasional (JKN) sejak tahun 2014 melalui badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan. Kebijakan ini merupakan wujud komitmen negara dalam merealisasikan Universal Health Coverage (UHC), yang secara yuridis berlandaskan pada Undang-Undang Nomor 40 Tahun 2004 tentang Sistem Jaminan Sosial Nasional serta Undang-Undang Nomor 24 Tahun 2011 tentang Badan Penyelenggara Jaminan Sosial (Azmi et al., 2024).

Seiring dengan berkembangnya sistem layanan kesehatan, transformasi digital juga mulai memainkan peran penting dalam mendukung pengelolaan layanan kesehatan, termasuk dalam sistem jaminan kesehatan nasional. Perkembangan teknologi digital yang berlangsung sangat cepat telah membawa perubahan signifikan di berbagai sektor, termasuk sektor kesehatan. Transformasi digital kini tidak hanya dipandang sebagai bentuk inovasi, tetapi telah menjadi elemen fundamental dalam pembaruan sistem pelayanan kesehatan secara menyeluruh, mencakup proses administrasi, pola interaksi antara pasien dan tenaga kesehatan, serta pengelolaan data kesehatan yang semakin kompleks. Penerapan teknologi digital seperti kecerdasan buatan, Internet of Things, dan layanan telemedicine berkontribusi dalam meningkatkan efisiensi operasional serta kualitas pelayanan kesehatan (Manurung & Simarmata, 2025). Dalam konteks asuransi kesehatan, BPJS Kesehatan sebagai penyelenggara jaminan kesehatan nasional mengelola berbagai data sensitif peserta, termasuk data pribadi, data kesehatan, dan data keuangan. Pengelolaan data tersebut menghadapi berbagai tantangan keamanan siber, seperti risiko kebocoran, penyalahgunaan, dan akses tidak sah terhadap informasi peserta. Salah satu kasus yang menjadi perhatian publik adalah dugaan kebocoran data BPJS Kesehatan pada tahun 2021 yang melibatkan jutaan data pribadi masyarakat Indonesia. Peristiwa tersebut menunjukkan pentingnya penerapan sistem keamanan data yang kuat karena kegagalan dalam melindungi data tidak hanya menimbulkan risiko penyalahgunaan informasi, tetapi juga dapat menurunkan tingkat kepercayaan masyarakat terhadap institusi penyedia layanan kesehatan digital (Panggabean & Fitria, 2025).

Temuan ini sejalan dengan tren global yang menunjukkan bahwa sektor kesehatan dengan tingkat pelanggaran data tertinggi secara global. Ribuan kasus pelanggaran terkonfirmasi dalam periode 2005–2019, dengan insiden peretasan sebagai penyebab utama dan tren yang terus meningkat secara signifikan (Seh et al., 2020). Kondisi ini mempertegas bahwa keamanan dan privasi data merupakan determinan penting dalam membangun dan menjaga kepercayaan publik terhadap sistem layanan kesehatan berbasis teknologi (Belfrage et al., 2022). Namun demikian, sebagian besar literatur mengenai digitalisasi layanan kesehatan masih berfokus pada peningkatan efisiensi dan kualitas layanan, sementara kajian yang membahas aspek keamanan data dan kepercayaan publik cenderung dilakukan secara terpisah dan belum terintegrasi secara komprehensif dalam konteks asuransi kesehatan. Hingga saat ini, belum banyak kajian yang secara spesifik mengintegrasikan aspek keamanan data dan kepercayaan publik dalam konteks digitalisasi asuransi kesehatan di Indonesia. Kondisi ini menunjukkan bahwa keterkaitan antara keamanan data dan kepercayaan publik dalam proses digitalisasi asuransi kesehatan masih memerlukan penelitian yang lebih mendalam. Kajian ini berfokus pada pembahasan tantangan keamanan data dalam digitalisasi asuransi kesehatan serta implikasinya terhadap kepercayaan publik.

METODE

Penelitian ini menggunakan metode deskriptif-analitis dengan pendekatan studi literatur (*literature review*). Data dikumpulkan melalui penelusuran komprehensif terhadap berbagai literatur ilmiah menggunakan kata kunci dalam bahasa Indonesia dan Inggris, yaitu "Digitalisasi", "Keamanan Data", "Kepercayaan Publik", "Privasi", "Siber", dan "Tata Kelola Data". Penelusuran dilakukan pada beberapa basis data akademik, antara lain Google Scholar, Garuda,

BMC, Frontiers dan Wiley Online Library dengan fokus pada publikasi dalam rentang tahun 2020-2026 untuk memastikan kebaruan dan relevansi informasi.

Proses seleksi dilakukan melalui tahap identifikasi, penyaringan, dan penilaian kelayakan berdasarkan kriteria inklusi dan eksklusi yang telah ditetapkan, seperti kesesuaian topik dengan fokus penelitian, jenis publikasi berupa artikel ilmiah peer-reviewed, serta ketersediaan teks lengkap. Artikel yang tidak relevan, duplikasi, atau tidak memenuhi standar kualitas dieliminasi. Setelah proses seleksi, sebanyak sepuluh artikel terpilih untuk dianalisis lebih lanjut. Analisis dilakukan secara tematik dengan mengkaji risiko keamanan, perlindungan privasi, serta faktor-faktor yang memengaruhi kepercayaan publik dalam ekosistem asuransi digital. Metode ini bertujuan untuk memperoleh pemahaman yang komprehensif mengenai tantangan keamanan data dalam digitalisasi asuransi kesehatan serta implikasinya terhadap kepercayaan publik.

HASIL DAN PEMBAHASAN

Tabel 1. Hasil Kajian Artikel Keamanan Data dan Kepercayaan Publik dalam Digitalisasi Asuransi Kesehatan di Indonesia

Nomor	Penulis/Tahun	Judul	Metode	Hasil
1	Hana Nur Hanifah & Arista Candra Irawati (2024)	Urgensi *Cyber Law* dalam Menjaga Privasi Pasien di Rumah Sakit Era Digital	Penelitian Analisis Data	Digitalisasi kesehatan menghadapi risiko keamanan serius berupa kejahatan siber (pencurian data dan akses ilegal) yang diperburuk oleh kesenjangan infrastruktur teknologi serta tingginya volume data pasien. Dari sisi privasi, transisi ke sistem elektronik membuka celah pencurian identitas dan kebocoran informasi sensitif. Masalah utama terletak pada aspek etika, rendahnya literasi hukum tenaga kesehatan, dan ancaman terhadap kepercayaan publik, sehingga implementasi *cyber law* menjadi krusial untuk melindungi kerahasiaan data pasien.

2	Enno Karina Fandayani (2026)	Analisis Perlindungan Data Medis Nasabah di Perusahaan Asuransi Jiwa	Kualitatif (Deskriptif-Analitis)	Digitalisasi asuransi jiwa melalui sistem Rekam Medis Elektronik (RME) membawa tantangan teknologi berupa risiko kebocoran data yang diperparah oleh keterbatasan kapasitas SDM dan ketergantungan pada pihak ketiga dalam pengelolaan IT. Data medis merupakan informasi sangat sensitif yang jika bocor dapat menimbulkan kerugian multidimensional, baik secara material, psikologis, maupun sosial. Penelitian ini juga menyoroti adanya ketidakoptimalan kebijakan internal akibat belum adanya standar operasional yang seragam di tingkat industri asuransi dalam melindungi privasi data medis.
3	Indah Susilowati, Lia Agustina & Ratna Frenty Nurkhalim (2025)	Edukasi Mengenai Upaya Menjaga Privasi Data Pribadi Dalam Penggunaan *E-Health*	Pengabdian Masyarakat (Sosialisasi, Wawancara, dan Tanya Jawab)	Digitalisasi layanan kesehatan (*e-health*) meningkatkan risiko keamanan yang bersumber dari kelalaian manusia seperti penggunaan kata sandi lemah, serta memicu kejahatan siber berupa pencurian identitas dan penipuan klaim asuransi. Transaksi tanpa tatap muka juga memperlemah perlindungan kerahasiaan data. Dari aspek privasi, ditemukan ancaman eksploitasi data kesehatan di forum daring dan risiko diskriminasi medis terhadap individu. Hasil kegiatan menunjukkan bahwa rendahnya literasi privasi masyarakat menjadi faktor utama kerentanan data pribadi, sehingga diperlukan peningkatan kesadaran mengenai hak dan tanggung jawab dalam menggunakan platform digital.

4	Narongsak Sukma & Siriporn Yamnill (2025)	*A New Public Management Model for Open Data Collaboration in Sustainable Digital Insurance Ecosystems*	Analisis *Structural Equation Modeling* (SEM) dengan 368 profesional (regulator, industri, teknologi).	Ekspektasi kinerja adalah prediktor terkuat niat perilaku. Keterlibatan berprinsip melalui berbagi data terbuka (*open data*) memiliki pengaruh lebih kuat terhadap hasil berkelanjutan daripada sekadar adopsi teknologi.
5	Narongsak Sukma & Siriporn Yamnill (2025)	*Trust, Commitment, and Technology: An Integrated Model of Collaborative Governance in Digital Insurance Regulation*	*Structural Equation Modeling* (PLS-SEM) dengan data dari 546 pemangku kepentingan	Faktor relasional (kepercayaan dan komitmen) memediasi hubungan antara kapabilitas teknologi dan hasil kolaboratif. Solusi teknologi saja tidak cukup tanpa mekanisme pembangunan hubungan untuk kerja sama jangka panjang.
6	Gurucharann Visagamurthy (2025)	*Digitizing Trust: Ethical Dimensions of InsurTech in the Era of Financial Inclusion*	Analisis kualitatif/artikel penelitian mengenai dimensi etika.	Digitalisasi operasional asuransi mengubah dinamika akses. Kepercayaan digital sangat bergantung pada kerangka tata kelola yang kuat untuk menyeimbangkan inovasi dengan perlindungan data dan privasi.
7	Madhu Acharyya & Kayleb Butterfield (2025)	*Adoption of IoT-Based Insurance Solutions: Comparative Evidence from Health, Motor, and Home Sectors*	Survei kuantitatif (87 responden) menggunakan model UTAUT dan analisis SEM.	Ekspektasi kinerja adalah prediktor terkuat untuk asuransi kesehatan. Kekhawatiran privasi tidak berpengaruh langsung secara independen, namun kegunaan yang dirasakan dapat mengurangi keraguan privasi tersebut.

8	Ameer Ahmed, dkk. (2025)	*Evaluating the effectiveness of data governance frameworks in ensuring security and privacy of healthcare data: A quantitative analysis of ISO standards, GDPR, and HIPAA in blockchain technology*	Kuantitatif (Survei 250 pakar kesehatan, IT, dan blockchain).	Kerangka kerja tradisional dinilai kurang memadai untuk teknologi terdesentralisasi. Penggunaan blockchain dengan *smart contracts* direkomendasikan untuk otomatisasi kepatuhan dan menjamin integritas data.
9	Marieke A. R. Bak, dkk. (2023)	*Towards trust-based governance of health data research*	Etika Empiris (Wawancara kualitatif 16 peneliti kesehatan).	Kepatuhan formal yang kaku berisiko memicu rutinisasi tanpa refleksi etis dan mengikis kepercayaan. Diusulkan tata kelola berbasis kepercayaan yang mengedepankan dialog demokratis dan transparansi.
10	Radovan Tomášik, dkk. (2026)	*Privacy-preserving data quality assessment for federated health data networks*	Kuantitatif (Eksperimen *Proof-of-Concept* pada dataset sintetik FHIR).	Implementasi teknik *differential privacy* terbukti efektif memungkinkan penilaian kualitas data secara terdesentralisasi tanpa mengekspos data mentah. Penggunaan noise (gangguan) terkontrol melindungi privasi individu sambil tetap memberikan metrik kualitas yang akurat.

Sumber: Data Sekunder

Risiko Keamanan dan Privasi Data dalam Digitalisasi Asuransi Kesehatan

Digitalisasi asuransi kesehatan menghadirkan berbagai risiko keamanan yang berkaitan dengan aspek teknologi, sumber daya manusia, dan tata kelola sistem. Ancaman kejahatan siber seperti pencurian data, akses ilegal, serangan digital, pencurian identitas, pemerasan, hingga penipuan berbasis klaim asuransi menjadi tantangan utama dalam pengelolaan data kesehatan (Hanifah & Irawati, 2024; Susilowati et al., 2025). Risiko tersebut semakin meningkat akibat keterbatasan infrastruktur keamanan, tingginya mobilitas data pasien dalam sistem elektronik, penggunaan Rekam Medis Elektronik (RME), serta ketergantungan pada pihak ketiga dalam pengelolaan teknologi informasi (Fandayani, 2026). Selain itu, faktor *human error*, seperti penggunaan kata sandi yang lemah, kelalaian menjaga kerahasiaan informasi, dan rendahnya kepatuhan terhadap protokol keamanan, turut memperbesar peluang terjadinya kebocoran data (Susilowati et al., 2025).

Dari perspektif privasi, transformasi dari sistem manual ke sistem digital membuka peluang lebih besar terhadap pencurian identitas dan penyalahgunaan informasi kesehatan pasien. Perlindungan data medis merupakan upaya hukum, teknis, dan administratif untuk

menjaga kerahasiaan, integritas, dan ketersediaan informasi kesehatan sehingga data hanya digunakan untuk tujuan yang sah dan dengan persetujuan pemilik data (Frahma, 2024). Namun, rendahnya literasi hukum tenaga kesehatan terkait perlindungan data pribadi masih menjadi faktor yang meningkatkan risiko pelanggaran privasi (Hanifah & Irawati, 2024). Kebocoran data medis, seperti diagnosis, riwayat penyakit, hasil pemeriksaan laboratorium, dan tindakan medis, dapat menimbulkan dampak multidimensional berupa kerugian material, psikologis, maupun sosial. Kondisi ini diperburuk oleh belum adanya standar perlindungan data yang seragam antarperusahaan sehingga tingkat keamanan data medis masih bervariasi (Fandayani, 2026).

Untuk meminimalkan risiko tersebut, penerapan konsep *Privacy by Design* menjadi salah satu strategi yang penting dalam pengelolaan data medis. Pendekatan ini mengintegrasikan perlindungan privasi sejak tahap perencanaan, pengembangan, hingga operasional sistem dengan menjadikan privasi sebagai pengaturan bawaan (*default privacy*). Selain memastikan keamanan pada seluruh siklus hidup data, mulai dari pengumpulan, pengolahan, penyimpanan, hingga pemusnahan, *Privacy by Design* juga mendorong transparansi dan memberikan kendali yang lebih besar kepada pemilik data atas penggunaan informasi pribadinya (Laraswati et al., 2025). Penerapan pendekatan ini menjadi semakin relevan dalam ekosistem digital asuransi kesehatan yang melibatkan berbagai pihak dan pertukaran data secara berkelanjutan. Di samping itu, meningkatnya risiko eksploitasi data kesehatan dan rendahnya literasi privasi masyarakat menunjukkan perlunya penguatan edukasi serta tata kelola perlindungan data untuk mencegah penyalahgunaan informasi kesehatan pribadi (Susilowati et al., 2025).

Hubungan Keamanan Data dengan Kepercayaan Publik dan Adopsi Layanan Digital

Transformasi digital dalam industri asuransi mendorong pemanfaatan teknologi seperti kecerdasan buatan, analitik data, dan berbagai platform digital untuk meningkatkan efisiensi layanan serta pengalaman pelanggan. Salah satu perkembangan yang muncul adalah konsep *open insurance*, yaitu pertukaran data asuransi melalui teknologi seperti Application Programming Interface (API) yang memungkinkan inovasi layanan yang lebih personal dan terintegrasi. Namun, penggunaan data dalam sistem digital juga menimbulkan tantangan terkait perlindungan privasi dan keamanan data pengguna. Oleh karena itu, tata kelola data yang kuat diperlukan untuk memastikan bahwa inovasi digital dalam industri asuransi tetap sejalan dengan perlindungan konsumen dan keamanan informasi (Sukma & Yamnill, 2025a).

Penelitian oleh Sukma dan Yamnill (2025) menunjukkan bahwa keberhasilan ekosistem asuransi digital tidak hanya bergantung pada penerapan teknologi, tetapi juga pada keterlibatan yang baik antar pemangku kepentingan. Studi tersebut menemukan bahwa niat masyarakat untuk mengadopsi layanan *open insurance* dipengaruhi oleh ekspektasi kinerja (*performance expectancy*), yaitu ketika pengguna merasakan manfaat nyata seperti efisiensi dan transparansi layanan. Selain itu, akuntabilitas dalam pengelolaan data menjadi faktor penting dalam membangun dan mempertahankan kepercayaan publik terhadap layanan asuransi digital (Sukma & Yamnill, 2025a).

Selain faktor manfaat bagi pengguna, Sukma dan Yamnill (2025) dalam studi lainnya juga menekankan bahwa keberlanjutan ekosistem asuransi digital tidak hanya bergantung pada kemampuan teknologi, tetapi juga pada komitmen serta kepercayaan antara sektor publik dan swasta. Hasil studi tersebut menunjukkan bahwa teknologi tidak akan memberikan dampak maksimal tanpa adanya kepercayaan dan komitmen jangka panjang dalam tata kelola kolaboratif. Oleh karena itu, keamanan data tidak hanya dipahami sebagai aspek teknis, tetapi juga sebagai hasil dari transparansi dan koordinasi yang kuat antara penyedia layanan asuransi dan regulator dalam mengelola risiko digital (Sukma & Yamnill, 2025b).

Visagamurthy (2025) menekankan bahwa digitalisasi dalam industri asuransi perlu disertai dengan penerapan prinsip etika untuk menjaga kepercayaan publik. Penelitian tersebut menunjukkan bahwa inovasi seperti algoritma *underwriting real-time* dan platform data yang saling terhubung memerlukan tata kelola yang etis guna mencegah bias serta melindungi privasi data pengguna. Oleh karena itu, kepercayaan terhadap layanan digital tidak hanya bergantung pada kecanggihan teknologi atau kerja sama antar lembaga, tetapi juga pada komitmen perusahaan asuransi dalam menerapkan desain yang berpusat pada pengguna serta akuntabilitas algoritma agar layanan tetap adil bagi masyarakat (Visagamurthy, 2025).

Penelitian Acharyya dan Butterfield (2025) memberikan gambaran empiris mengenai adopsi teknologi Internet of Things (IoT) dalam asuransi kesehatan. Hasil studi tersebut menunjukkan bahwa meskipun isu privasi data menjadi perhatian, ekspektasi kinerja (*performance expectancy*) tetap menjadi faktor utama yang mempengaruhi niat pengguna dalam mengadopsi layanan digital. Selain itu, manfaat yang dirasakan dari penggunaan perangkat digital dapat mengurangi kekhawatiran pengguna terhadap risiko privasi. Temuan ini menunjukkan bahwa kepercayaan publik tidak hanya dibangun melalui keamanan teknis dan aspek etika, tetapi juga melalui manfaat nyata yang dirasakan oleh pengguna (Acharyya & Butterfield, 2025). Dengan demikian, Keamanan data dan tata kelola informasi yang baik menjadi faktor penting dalam membangun kepercayaan publik terhadap layanan asuransi digital. Tingkat kepercayaan tersebut pada akhirnya dapat mempengaruhi keputusan masyarakat untuk mengadopsi dan menggunakan layanan digital.

Praktik Tata Kelola untuk Memperkuat Keamanan Data dan Kepercayaan Publik

Implementasi digitalisasi asuransi kesehatan menuntut transformasi tata kelola yang tidak hanya berfokus pada kepatuhan hukum, tetapi juga pada keandalan teknologi dan aspek kemanusiaan. Praktik tata kelola yang kuat dimulai dengan integrasi teknologi mutakhir seperti *blockchain* untuk mengatasi keterbatasan kerangka kerja tradisional dalam ekosistem desentralisasi. Penggunaan *smart contracts* dalam sistem *blockchain* memungkinkan otomatisasi kepatuhan terhadap regulasi, di mana akses terhadap data hanya diberikan berdasarkan kondisi yang telah ditentukan sebelumnya, sehingga menjamin integritas data dan transparansi jejak audit (Ahmed et al., 2025).

Selain aspek struktural, efektivitas tata kelola sangat bergantung pada perlindungan privasi selama proses evaluasi kualitas data. Penggunaan teknik *differential privacy* menjadi praktik krusial dalam jaringan data kesehatan terfederasi. Metode ini memungkinkan penyedia data untuk menghitung metrik kualitas secara lokal dan hanya membagikan hasil agregat yang telah diberi gangguan (*noise*) terkontrol. Hal ini memastikan bahwa informasi sensitif individu tidak terekspos selama proses analisis, yang pada gilirannya memperkuat keamanan data tanpa mengurangi kegunaan informasi untuk pengambilan keputusan (Tomášik et al., 2026).

Namun, tata kelola yang terlalu kaku dan hanya berorientasi pada pemenuhan daftar periksa (*checkbox exercise*) formalitas hukum berisiko menyebabkan rutinisasi di kalangan peneliti. Kondisi ini dapat mengikis kepercayaan antar-aktor dalam ekosistem data kesehatan jika refleksi etis dikesampingkan demi kepatuhan administratif semata (Bak et al., 2023). Kesenjangan ini mempertegas pentingnya dimensi etika dalam operasional teknologi asuransi (*InsurTech*), di mana kepercayaan digital tidak dapat bertumpu pada kecanggihan teknologi semata, melainkan pada kerangka tata kelola etis yang kuat. Tata kelola tersebut harus mampu menyeimbangkan inovasi layanan dengan jaminan privasi melalui transparansi sistem penanganan model algoritma yang proaktif terhadap isiko diskriminasi data nasabah (Visagamurthy, 2025).

Oleh karena itu, diperlukan model tata kelola berbasis kepercayaan (*trust-based governance*) yang mengedepankan dialog demokratis dan keterlibatan publik. Membangun "tag kepercayaan" (*trust-tags*) melalui transparansi kebijakan dan penjelasan terbuka mengenai

mekanisme pengawasan menjadi langkah strategis untuk menjaga kontrak sosial antara pengelola data dan masyarakat (Bak et al., 2023). Melalui akuntabilitas algoritma yang berorientasi pada pengguna (*human-centered design*) serta pengawasan yang kolaboratif, transparansi pengolahan data sensitif dapat memulihkan kepercayaan konsumen ketika terjadi ketidakpastian dalam sistem tata kelola digital (Visagamurthy, 2025). Dengan mengintegrasikan keamanan teknis melalui *blockchain*, perlindungan privasi melalui *differential privacy*, dan pendekatan etis berbasis kepercayaan, institusi asuransi dapat menciptakan lingkungan digital yang aman sekaligus memenangkan kepercayaan publik secara berkelanjutan.

PENUTUP

Simpulan

Digitalisasi asuransi kesehatan melalui JKN berperan penting dalam mendukung pencapaian UHC di Indonesia. Namun, implementasinya masih menghadapi berbagai tantangan keamanan data, baik dari aspek teknologi maupun sumber daya manusia. Kerentanan sistem dipengaruhi oleh keterbatasan infrastruktur, ketergantungan pada pihak ketiga, *human error*, serta rendahnya literasi privasi dan hukum. Selain itu, kepercayaan publik terhadap asuransi digital sangat bergantung pada manfaat yang dirasakan pengguna, akuntabilitas algoritma, dan transparansi tata kelola data.

Saran

Penyelenggara asuransi kesehatan digital perlu mengadopsi teknologi yang lebih inovatif, seperti *blockchain* dan *smart contracts*, untuk meningkatkan keamanan serta kepatuhan pengelolaan data. Penggunaan *differential privacy* juga perlu dipertimbangkan untuk menjaga kerahasiaan data individu. Selain itu, tata kelola data sebaiknya dikembangkan menuju pendekatan berbasis kepercayaan (*trust-based governance*) yang menekankan transparansi, akuntabilitas, dan komitmen etis dalam jangka panjang.

DAFTAR PUSTAKA

Acharyya, M., & Butterfield, K. (2025). Adoption of IoT-Based Insurance Solutions: Comparative Evidence from Health, Motor, and Home Sectors. https://doi.org/http://dx.doi.org/10.2139/ssrn.5395140

Ahmed, A., Shahzad, A., Naseem, A., Ali, S., & Ahmad, I. (2025). Evaluating the effectiveness of data governance frameworks in ensuring security and privacy of healthcare data: A quantitative analysis of ISO standards, GDPR, and HIPAA in blockchain technology. *PLoS ONE*, 20(5), 1–18. https://doi.org/10.1371/journal.pone.0324285

Azmi, F., Zulvita Rahayu, B., & Hidayatullah, D. (2024). ANALISIS EFEKTIVITAS PROGRAM ASURANSI KESEHATAN NASIONAL DALAM MENINGKATKAN AKSES PELAYANAN KESEHATAN DI INDONESIA. *JURNAL KESEHATAN TAMBUSAI,* 5(4), 13667–13677. https://doi.org/10.31004/jkt.v5i4.35895

Bak, M. A. R., Ploem, M. C., Tan, H. L., Blom, M. T., & Willems, D. L. (2023). Towards trust-based governance of health data research. *Medicine, Health Care and Philosophy,* 26(2), 185–200. https://doi.org/10.1007/s11019-022-10134-8

Belfrage, S., Helgesson, G., & Lynøe, N. (2022). Trust and digital privacy in healthcare: a cross-sectional descriptive study of trust and attitudes towards uses of electronic health data among the general public in Sweden. *BMC Medical Ethics*, 23(19). https://doi.org/10.1186/s12910-022-00758-z

Fandayani, K. E. (2026). ANALISIS PERLINDUNGAN DATA MEDIS NASABAH DI PERUSAHAAN ASURANSI JIWA. *COSTING: Journal of Economic, Business and Accounting*, 9(1), 2224–2231. ttps://doi.org/10.31539/40k96666

Frahma, A. E. (2024). JURIDICAL ANALYSIS OF PATIENT DATA PROTECTION IN NATIONAL LEGAL PERSPECTIVE. *UNTAG Law Review (ULREV),* 8(1), 399–423. https://doi.org/http://jurnal.untagsmg.ac.id/indeks.php/ulrev/indeks

Hanifah, N. H., & Irawati, C. A. (2024). URGENSI CYBER LAW DALAM MENJAGA PRIVASI PASIEN DI RUMAH SAKIT ERA DIGITAL. *Adil Indonesia Journal,* 5, 154–161. https://doi.org/https://doi.org/10.35473/aij.v5i2.3945

Laraswati, D., Khadaffy, M., Hakim, A. E., Subekti, K. A., Nurvika, N., & Royadih tyas Alfarizza, A. (2025). Analisis Konseptual Penerapan Privacy-by-Design dalam Perlindungan Informasi Pribadi. *Jurnal Pendidikan Tambusai*, 9(3), 38616–38620. https://doi.org/https://doi.org/10.31004/jptam.v9i3.34811

Manurung, R. I. P., & Simarmata, M. (2025). Digitalisasi Layanan Kesehatan: Tantangan Etika dan Keamanan Data Pasien. *Presidensial: Jurnal Hukum, Administrasi Negara, Dan Kebijakan Publik*, 2(2), 263–273. https://doi.org/10.62383/presidensial.v2i2.811

Panggabean, M. V., & Fitria, A. (2025). Perlindungan Hukun Data Pribadi di Indonesia (Kasus Kebocoran Badan Penyelengara Jaminan Sosial Kesehatan). *Arus Jurnal Sosial Dan Humaniora (AJSH)*, 5(2), 1958–1965. https://doi.org/http://jurnal.ardenjaya.com/index.php/ajsh

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. *In Healthcare (Switzerland)* 8(2), pp. 1–18. MDPI AG. https://doi.org/10.3390/healthcare8020133

Sukma, N., & Yamnill, S. (2025a). A new public management model for open data collaboration in sustainable digital insurance ecosystems. *Frontiers in Political Science*, 7. https://doi.org/10.3389/fpos.2025.1598403

Sukma, N., & Yamnill, S. (2025b). Trust, Commitment, and Technology: An Integrated Model of Collaborative Governance in Digital Insurance Regulation. *Human Behavior and Emerging Technologies*, (8884386), 29. https://doi.org/10.1155/hbe2/8884386

Susilowati, I., Agustina, L., & Nurkhalim Frenty, R. (2025). Edukasi Mengenai Upaya Menjaga Privasi Data Pribadi Dalam Penggunaan E-Health. *Journal of Community Enggagement and Empowerment (JCEE),* 7(1), 63–69. https://doi.org/http://ojs.iik.ac.id/index.php/JCEE

Tomášik, R., Kussel, T., Dudová, Z., Kacová, R., Hrstka, R., Lablans, M., & Holub, P. (2026). Privacy-preserving data quality assessment for federated health data networks. *BMC Medical Informatics and Decision Making*, 26(1), 1–11. https://doi.org/10.1186/s12911-025-03328-6

Visagamurthy, G. (2025). Digitizing Trust: Ethical Dimensions of InsurTech in the Era of Financial Inclusion. *Journal of Computer Science and Technology Studies.* https://doi.org/DOI:10.32996/jcsts.2025.7.5.116