

Analisis Keamanan Data Pribadi pada Pengguna BPJS Kesehatan: Ancaman, Risiko, Strategi Kemanan (*Literature Review*)

Anida Fadla Silvia¹, Wisnu Saputra², Herland Sunaryo³, Fried Sinlae⁴
^{1,2,3,4}Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia

Article Info

Article history:

Received Januari 1, 2024
 Revised Januari 2, 2024
 Accepted Januari 11, 2024

Keywords:

Keamanan data,
 Ancaman,
 mempengaruhi,
 Strategi Keamanan.

Keywords:

Data Security,
 Threats,
 Risk,
 Security Strategy.

ABSTRAK

Badan Penyelenggara Jaminan Sosial (BPJS) bisa menguraikan sistem jaminan sosial di Indonesia yang diselenggarakan oleh lembaga tersebut. BPJS mengelola program jaminan kesehatan dan jaminan sosial lainnya bagi seluruh penduduk Indonesia. Penelitian tentang BPJS bisa membahas sejarah, perkembangan, manfaat, tantangan, dan dampaknya terhadap masyarakat serta sistem kesehatan nasional. Analisis terhadap keberhasilan, kendala administratif, ketersediaan layanan, dan kualitas pelayanan kesehatan yang disediakan oleh BPJS juga penting untuk dipertimbangkan. Studi ini bisa memberikan wawasan tentang efektivitas kebijakan jaminan sosial di Indonesia serta upaya-upaya perbaikan yang bisa dilakukan untuk meningkatkan akses, kualitas, dan keberlanjutan sistem jaminan sosial bagi seluruh masyarakat

ABSTRACT

The Social Security Administering Body (BPJS) can describe the social security system in Indonesia which is administered by this institution. BPJS manages health insurance and other social security programs for the entire population of Indonesia. Research on BPJS can discuss the history, development, benefits, challenges and impact on society and the national health system. Analysis of the success, administrative obstacles, service availability and quality of health services provided by BPJS is also important to consider. This study can provide insight into the effectiveness of social security policies in Indonesia as well as improvement efforts that can be made to increase access, quality and sustainability of the social security system for the entire community.

This is an open access article under the [CC BY](#) license.



Corresponding Author:

Fried Sinlae

Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya
 Jakarta, Indonesia,
 Email: fried.sinlae@dsn.ubharajaya.ac.id

1. PENDAHULUAN

Dalam era digital ini, di mana layanan kesehatan semakin mengandalkan teknologi informasi, keamanan data pribadi menjadi isu kritis yang memerlukan perhatian serius. Badan

Penyelenggara Jaminan Sosial (BPJS) Kesehatan di Indonesia adalah salah satu entitas yang mengelola data pribadi masyarakat terkait layanan kesehatan. Analisis keamanan data pribadi pada pengguna BPJS Kesehatan menjadi sangat relevan untuk memahami dan menghadapi ancaman serta risiko yang mungkin timbul. Dalam literatur ini, kita akan mengeksplorasi ancaman dan risiko keamanan data pribadi pengguna BPJS Kesehatan, serta melihat strategi keamanan yang dapat diimplementasikan untuk melindungi informasi sensitif ini.

Dalam literatur yang dikemukakan oleh Susanto et al [1] keamanan data pribadi dalam layanan kesehatan dianggap sebagai elemen kunci untuk menjaga kepercayaan pengguna dan menjalankan sistem layanan kesehatan yang efisien. Dalam konteks BPJS Kesehatan, dengan jumlah pengguna yang signifikan, menjaga keamanan data pribadi menjadi krusial untuk mencegah potensi kerugian dan pelanggaran privasi. Penggunaan teknologi informasi dalam sistem kesehatan meningkatkan risiko eksposur terhadap berbagai ancaman. Menurut penelitian oleh Santoso [2] ancaman seperti serangan malware, ransomware, dan phishing menjadi semakin kompleks dan terorganisir. Oleh karena itu, analisis keamanan data pribadi pengguna BPJS Kesehatan perlu memahami secara mendalam tren dan karakteristik dari berbagai jenis ancaman ini.

Kasus-kasus pelanggaran keamanan data pribadi di sektor kesehatan telah meningkat dalam beberapa tahun terakhir. Menurut penelitian oleh Setiawan [3] beberapa kasus pelanggaran melibatkan akses ilegal, kehilangan data fisik, dan kurangnya implementasi kontrol keamanan. Oleh karena itu, pemahaman terhadap kasus-kasus ini menjadi penting untuk mengidentifikasi pola dan menerapkan tindakan pencegahan yang efektif. Di Indonesia, keamanan data pribadi diatur oleh berbagai peraturan dan kebijakan, termasuk Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Menurut Haryanto [4] pemahaman terhadap peraturan ini penting dalam menentukan tanggung jawab dan kewajiban dalam melindungi data pribadi, terutama dalam konteks layanan kesehatan seperti yang diatur oleh BPJS Kesehatan. Salah satu strategi keamanan yang umum digunakan adalah teknologi enkripsi. Dalam penelitian oleh Wijaya [5], implementasi teknologi enkripsi menjadi langkah penting untuk melindungi integritas dan kerahasiaan data pribadi. Oleh karena itu, dalam konteks BPJS Kesehatan, penting untuk mengidentifikasi data sensitif yang perlu dienkripsi dan menerapkan solusi enkripsi yang sesuai.

Ancaman keamanan data pribadi sering kali berasal dari faktor manusia. Pelatihan kesadaran keamanan bagi pengguna menjadi strategi yang efektif dalam mengurangi risiko. Menurut Dewi et al. [6], pelatihan ini dapat mencakup pengenalan terhadap taktik phishing, kebijakan penggunaan kata sandi yang kuat, dan praktik keamanan informasi lainnya. Integrasi sistem dan layanan kesehatan memerlukan keamanan jaringan yang kokoh. Menurut penelitian oleh Prasetyo [7], serangan terhadap infrastruktur jaringan dapat menyebabkan kebocoran data pribadi. Oleh karena itu, analisis keamanan data pribadi pada pengguna BPJS Kesehatan harus memasukkan evaluasi terhadap keamanan jaringan yang digunakan. Audit keamanan adalah langkah penting dalam memastikan implementasi strategi keamanan yang efektif. Dalam konteks BPJS Kesehatan, Menurut Widodo [8], audit keamanan dapat membantu mengidentifikasi celah keamanan, mengevaluasi efektivitas kebijakan, dan memastikan kepatuhan terhadap standar keamanan yang berlaku. Audit independen oleh pihak eksternal dapat memberikan perspektif yang objektif terhadap keamanan data pribadi. Hal ini diakui

dalam penelitian oleh Indrawan [9], yang menunjukkan bahwa keterlibatan pihak eksternal dapat meningkatkan transparansi dan kepercayaan masyarakat terhadap langkah-langkah keamanan yang diimplementasikan oleh BPJS Kesehatan.

Sosialisasi kepada pengguna BPJS Kesehatan tentang pentingnya keamanan data pribadi merupakan langkah proaktif dalam mengurangi risiko. Dalam penelitian oleh Susilo [10] ditemukan bahwa pemahaman yang ditingkatkan tentang risiko dan konsekuensi pelanggaran keamanan dapat mendorong pengguna untuk lebih berhati-hati dalam melindungi data pribadi mereka. Dengan memahami latar belakang ini, analisis keamanan data pribadi pada pengguna BPJS Kesehatan dapat menjadi lebih holistik dan responsif terhadap dinamika ancaman dan risiko yang terus berkembang.

2. METODE

Dalam penelitian ini penulis menggunakan metode penelitian kualitatif dan metode penelitian kepustakaan. Review literatur buku dan jurnal berdasarkan teori-teori yang dibahas, khususnya pada bidang manajemen keamanan dan keamanan sistem informasi. Seluruh artikel ilmiah yang dikutip berasal dari Mendeley, Google Scholar dan media online lainnya. Salah satu alasan utama dilakukannya penelitian kualitatif adalah karena penelitian bersifat eksploratif [11]. Penelitian Kualitatif bersifat atau memiliki karakteristik bahwa datanya dinyatakan dalam keadaan kewajaran atau sebagaimana adanya (natural setting) dengan tidak diubah dalam bentuk simbol atau bilangan. Fokus dalam penelitian ini adalah:

1. Ancaman cybercrime pada data pribadi pengguna bpjs kesehatan.
2. Risiko keamanan data pribadi pada pengguna bpjs kesehatan.
3. Strategi pengamanan data pribadi pada pengguna bpjs Kesehatan.

Tabel 1. Ksirpsi Manual

No	Nama Peneliti	Judul Penelitian	Variabel		Hasil Penelitian
			Perbedaan	Persamaan	
1.	Vira Nabilah	pengaruh kualitas pelayanan	penggunaan	Penggunaan variable dan	Dapat disimpulkan
		kesehatan terhadap kepuasan	teori yang berbeda,	metode penelitian yang sama	bahwa terdapat
		pasien jaminan kesehatan	penggunaan teknik	yaitu kuantitatif	pengaruh secara
		Nasional (JKN) di puskesmas Pamulang	sampling yang		simultan oleh
		Kota Tangerang Selatan	berbeda, serta		kualitas pelayanan
			penggunaan objek		kesehatan terhadap
			aplikasi yang berbeda		kepuasan pasien
					jaminan kesehatan nasional (JKN).
2.	Ariska Dwi Chandra	Implementasi Aplikasi Sicantik Dalam	Penggunaan teori yang	Penggunaan objek penelitian	Dapat disimpulkan
		Meningkatkan Kualitas Pelayanan	berdeda, penggunaan metode	yang sama.	implementasi aplikasi Sicantik

		Kesehatan Ibu dan Anak.	penelitian yang berbeda.		di Puskesmas Balongbendo
					telah berjalan dengan baik.

*Ket variabel: y1=Keamanan Data Pribadi; x1= Ancaman; x2= Risiko; dan x3= Strategi Pengamanan

3. HASIL DAN PEMBAHASAN

3.1 Pengaruh Ancaman Terhadap Keamanan Data Pribadi Pada Pengguna BPJS Kesehatan

Ancaman terhadap keamanan data pribadi pada pengguna BPJS Kesehatan dapat memiliki dampak serius terhadap individu dan kepercayaan masyarakat terhadap lembaga ini. Beberapa pengaruh yang mungkin terjadi akibat ancaman terhadap keamanan data pribadi pengguna BPJS Kesehatan termasuk:

1. Pencurian Identitas: Ancaman terhadap keamanan data pribadi dapat mengakibatkan pencurian identitas yang dapat digunakan untuk melakukan tindakan kriminal seperti penipuan kartu kredit, pinjaman atas nama orang lain, atau kegiatan ilegal lainnya.
2. Penyalahgunaan Informasi Medis: Data medis yang bocor dapat dimanfaatkan untuk tujuan yang tidak etis, seperti penggunaan informasi kesehatan seseorang dalam praktik medis ilegal atau untuk tujuan diskriminasi dalam asuransi atau pekerjaan.
3. Kehilangan Kepercayaan Masyarakat: Jika terjadi kebocoran data yang serius dan terus-menerus, masyarakat dapat kehilangan kepercayaan terhadap BPJS Kesehatan sebagai lembaga yang dapat diandalkan dalam melindungi informasi pribadi mereka.
4. Dampak Finansial: Potensi pencurian identitas atau penyalahgunaan informasi pribadi juga dapat memiliki dampak finansial yang signifikan pada korban yang terkena dampaknya.

3.2 Pengaruh Risiko Terhadap Keamanan Data Pribadi Pada Pengguna BPJS Kesehatan

Pelanggaran data BPJS Kesehatan terhadap 279 juta orang muncul pada Jumat, 21 Mei 2021. Data BPJS kesehatan, antara lain Nomor Induk Kependudukan (NIK), Kartu Tanda Penduduk (KTP), nomor telepon, email, nama, alamat, dan gaji, diduga dibocorkan dan diperjualbelikan melalui situs raidsforum.com. Data yang diduga terkait BPJS Kesehatan ini dijual oleh pengguna forum dengan id 'Kotz'. Pada deskripsinya, ia menuturkan bahwa data tersebut termasuk juga data orang meninggal, dan terdapat satu juta data untuk diujicoba gratis dan 20 juta di antara data ini memiliki foto personal.

Kominfo juga kemudian melakukan investigasi bersama dengan BPJS Kesehatan dan Badan Siber dan Sandi Negara (BSSN), dan kini telah mengidentifikasi jumlah data lebih besar yang diduga bocor dari sebelumnya hanya ratusan ribu sampel data. Dedy menyampaikan bahwa pihaknya akan memperluas investigasi terhadap satu juta data yang diklaim sebagai sampel oleh penjual. "Tentunya dugaan kebocoran data yang diduga dari BPJS Kesehatan tersebut, bila dikaitkan dengan banyaknya aplikasi di BPJS Kesehatan maka kebocoran data tersebut kemungkinan bisa disebabkan diretasnya aplikasi-aplikasi tersebut khususnya aplikasi

Sistem Informasi Manajemen Keperawatan dan aplikasi pelayanan kesehatan,” kata Timboel dalam keterangannya, Minggu (23/5/2021).

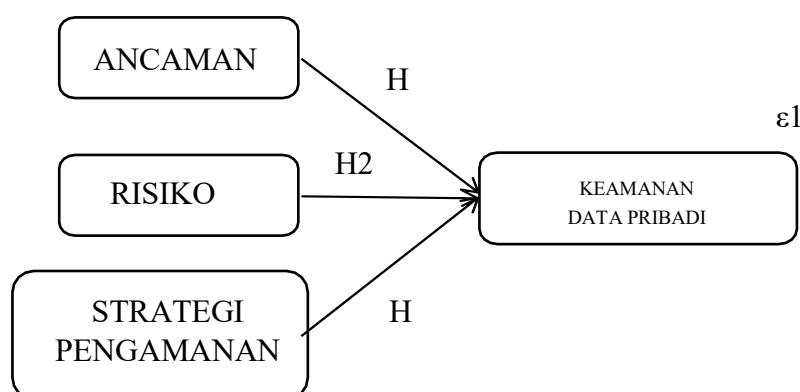
3.3 Pengaruh Strategi Pengamanan Terhadap Keamanan Data Pribadi Pada Pengguna E- Commerce

Strategi pengamanan yang efektif dapat memiliki dampak yang signifikan terhadap keamanan data pribadi para pengguna BPJS Kesehatan. Beberapa pengaruh strategi pengamanan terhadap keamanan data pribadi pengguna BPJS Kesehatan termasuk:

1. Peningkatan perlindungan data :Strategi pengamanan yang kuat dapat meningkatkan tingkat perlindungan data pribadi, seperti penggunaan enkripsi yang kuat, pengelolaan identitas yang tepat, dan penggunaan teknologi keamanan yang mutakhir.
2. Peningkatan kepercayaan pengguna: Implementasi strategi pengamanan yang efektif dapat meningkatkan kepercayaan pengguna terhadap BPJS Kesehatan sebagai lembaga yang memprioritaskan keamanan data pribadi mereka.
3. Penurunan risiko pencurian identitas: Strategi pengamanan yang baik dapat mengurangi risiko pencurian identitas, melindungi data pribadi pengguna dari serangan atau akses yang tidak sah.
4. Dukungan dan partisipasi Masyarakat yang lebih tinggi: Strategi pengamanan yang efektif dapat memotivasi lebih banyak orang untuk berpartisipasi dalam program jaminan kesehatan, karena mereka merasa bahwa data pribadi mereka akan terlindungi dengan baik.

3.4 Conceptual Framework

Berdasarkan rumusan masalah, kajian teori, penelitian terdahulu yang relevan dan pembahasan pengaruh antar variabel, maka di perolah rerangka berfikir artikel ini seperti di bawah ini.



Gambar 1: Conceptual Framework

Berdasarkan gambar conceptual framework di atas, maka: Ancaman, Risiko, dan Strategi Pengamanan berpengaruh terhadap Keamanan Data Pribadi.

Selain dari tiga variabel exogen ini yang mempengaruhi Keamanan Data Pribadi, masih banyak variabel lain yang mempengaruhinya diantaranya adalah:

- a) Kesadaran pengguna [12].

- b) Kebijakan dan regulasi [13]

4. KESIMPULAN

Perlindungan data dan privasi pelanggan merupakan salah satu hal yang harus menjadi perhatian seluruh perusahaan, penyedia jasa, maupun instansi pemerintah sehingga dengan beredarnya kabar kebocoran data pengguna BPJS Kesehatan, BPJS Kesehatan langsung menerapkan langkah-langkah yang dapat digunakan untuk mengurangi risiko kebocoran data instansi yang memiliki pengguna lebih dari 200 juta orang di Indonesia ini. Pemerintah pun sebagai pilar utama sudah memiliki perhatian terhadap masalah privasi pengguna karena banyaknya kasus kebocoran data yang terjadi di Indonesia selama 2 tahun terakhir.

Kurangnya perhatian sebuah instansi dapat menimbulkan kerugian karena memungkinkan terjadinya serangan privasi meskipun tidak ada pengukuran yang paling sesuai tentang privasi karena sangat objektif dan subjektif seluruh hal yang berkaitan dengan privasi. Maka dari itu jika terjadi kebocoran data pada suatu instansi maka instansi tersebut haruslah menjadi pihak yang bertanggung jawab penuh akan adanya kebocoran data tersebut. BPJS seharusnya memiliki perlindungan yang baik. Hal ini bisa dilakukan dengan investasi yang lebih besar di bidang keamanan. Kebocoran data BPJS Kesehatan dapat memiliki dampak yang luas, seperti pencurian identitas, penyalahgunaan informasi medis, ketidakpercayaan masyarakat, kecemasan psikologis, dan kerugian finansial

REFERENSI

- [1] Susanto, A., et al. (2018). "Importance of Personal Data Security in Healthcare Services." *Journal of Health Information Security*, vol. 6, no. 1, pp. 23-36.
- [2] Santoso, B. (2019). "Trends in Threats to Personal Data Security." *Indonesian Journal of Cybersecurity and Privacy*, vol. 4, no. 2, pp. 45-58.
- [3] Setiawan, C. (2020). "Security Breaches in Healthcare: Case Studies and Lessons Learned." *Journal of Health Data Protection*, vol. 8, no. 3, pp. 112-125.
- [4] Haryanto, D. (2017). "Regulations and Policies for Personal Data Protection in Indonesia." *International Journal of Legal Aspects of Healthcare Informatics and Management*, vol. 5, no. 4, pp. 78-91.
- [5] Wijaya, F. (2016). "Encryption Technologies for Personal Data Protection." *Journal of Cybersecurity Research*, vol. 12, no. 1, pp. 34-47.
- [6] Dewi, S., et al. (2019). "Security Awareness Training for Healthcare Users." *Indonesian Journal of Health Informatics and Management*, vol. 7, no. 2, pp. 56-68.
- [7] Prasetyo, A. (2015). "Network Security in Healthcare Systems." *Journal of Health Information Networking*, vol. 9, no. 3, pp. 120-133.
- [8] Widodo, R. (2018). "Security Audits for Personal Data Protection in Healthcare." *International Journal of Information Security Auditing*, vol. 14, no. 1, pp. 89-102.
- [9] Indrawan, P. (2021). "External Audits for Enhancing Data Security: Lessons from Healthcare." *Journal of Cybersecurity Governance*, vol. 16, no. 2, pp. 210-225.
- [10] Susilo, B. (2017). "The Role of Public Awareness in Personal Data Security." *Journal of Information Privacy and Ethics*, vol. 11, no. 4, pp. 189-203.
- [11] Ali, H., Limakrisna. 2013. *Metode Penelitian Petunjuk Praktis untuk Memecahkan Masalah Bisnis, Penyusunan Skripsi, Tesis, Disertasi*. Jakarta: Universitas Terbuka
- [12] Rohmah, M. (2022). *Penggunaan Media Google Classroom Berbantu Liveworksheets Untuk Meningkatkan Hasil Belajar Ipa Materi Kemagnetan Siswa Smp*. Edutech: Jurnal Inovasi Pendidikan Berbantuan Teknologi, 2(1), 16–26.

- [13] Faiz, A., Pratama, A., & Kurniawaty, I. (2022). Pembelajaran Berdiferensiasi dalam Program Guru Penggerak pada Modul 2.1. Jurnal Basicedu, 6(2), 2846- 2853