ALPHA MD®

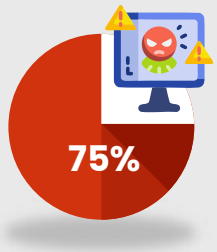
MONTHLY

NEWSLETTER

NOVEMBER 2025

HAVE YOU INSURED YOUR DATA ?

- Did you know a cyberattack happens every **39 seconds?**



- **75%** of cyber insurance claims from 2013-2019 were due to data breaches, incident response, and crisis management.
- The frequency of cyber insurance claim triggers is the **highest** for the healthcare industry, followed by IT and communications, Insurance, and Retail
- Claims increased by 100% over the past three years, while claims closed with payments rose by 200%, resulting in approximately 8,100 claims paid in 2021
- **Some thought-provoking questions:**
- **As an insurance provider, do you provide insurance cover to your customer data along with general insurance needs?**
- **What security protocols are followed while sharing data with Third party administrators ?**

Cyber Breaches in Indian Insurance Sector

Star Health and Allied Insurance: Largest breach in Indian health insurance history

In August 2024, Star Health and Allied Insurance suffered a catastrophic data breach affecting 31 million customers. Exposed data included Aadhaar numbers, PAN cards, medical reports, phone numbers, and addresses, all of which were reportedly sold on Telegram through automated bots and dark web channels for a mere $43,000.

HDFC Life Insurance (November 2024)

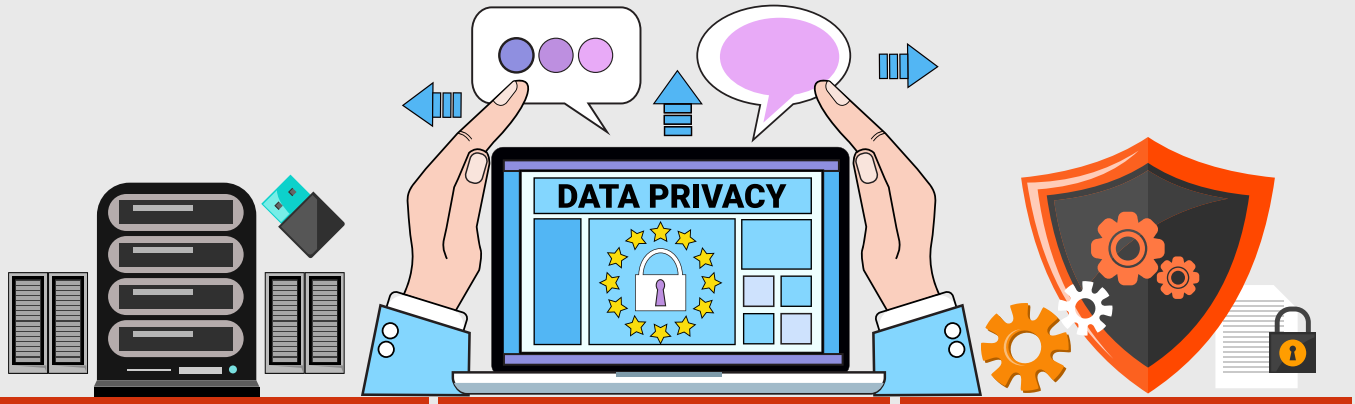
HDFC Life Insurance reported a data breach in November 2024. An unknown entity reportedly contacted the company, sharing certain customer data fields with alleged malicious intent.

In response, HDFC Life initiated an information security assessment and data log analysis to determine the breach's scope and implement remedial measures. Reports said, the company assured stakeholders that there was no material adverse impact from the incident.

Niva Bupa Health Insurance: A growing digital target

In February 2025, Niva Bupa Health Insurance, which covers 19.8 million lives, faced a significant cyber incident, when a threat actor claimed to have gained unauthorised access to customer data, publicly sharing select fields from two records with mala fide intent.

Insurance Data -Possible Weak Links



Insurance key functions	Data touch points	DPDP Rules Relevance
Proposal forms	Name. contact info, personal address	Lawful Consent, Provide clear and comprehensible notices at the time of admission. Include links for accessing policies on the website or digital health app
Claims forms	Name, Address, Age, Gender, contact info, medical condition, Hospitalization details, Hospitalization bills, Insured Bank account details	**Purpose Limitation** – Data must be used only for the purposes for which they are collected. **Data Minimization-** Only that Data must be collected from data principals which is required to accomplish the established purpose.
KYC	ID proofs Aadhar, Pan card	**Lawfulness** Sensitive Data processing should be undertaken on lawful grounds by Data Fiduciary. Consent for sharing data should be recorded and traceable. Patients should be able to view or revoke consent via as secure portal.
Medical Records	Lab Reports, X-rays , CT scan, Prescription, Hospital bills	Must deploy **appropriate security safeguards:** Encryption of medical records, Role-based access controls, Secure APIs for insurer–TPA data transfer.

ALPHA MD®

Preliminary Steps to DPDP Rules Compliance

Area of improvements	Actions taken	Methodology
Consent mechanism	Changes to the proposal forms, multilingual privacy notices	Management of consent process with explicit consent linked to each specific purpose.
Technology changes	Invest in tools as data discovery and data leakage prevention.	Incorporate practices like data anonymization, encryption and pseudonymisation
Third party arrangements	Additional Requirements to review TPA and ensure robust clauses around confidentiality, SLAs and penalties.	Governance mechanisms need to tightened. Periodic audits need to be planned to ensure personal data safeguards are in place.
Compliance monitoring	Classify the current data by building an inventory of personal data and create data flow . Data protection policy should be renewed in line with DPDP Act 's provisions.	Data protection officer to be appointed and made responsible for ensuring compliance with the provisions of the Act. Data privacy should be added as ongoing training programme and employees should be able to comprehend the data protection aspects and their implementation. Update Incident response and grievance mechanisms to cater to data breach requirements of the Data protection board.

OIDPM

ORCHA INDIA DATA PROTECTION MARK simplifies **DPDP Rules** compliance by helping businesses navigate complex data privacy regulations, ensuring seamless compliance and robust data security.

Source: Optima Insurance Brokers Pvt. Ltd. Available at: https://optima.co.in/cyber-onslaught-on-indias-insurance-sector-in-fy-25-a-wake-up-call/ (Accessed: 26 November 2025)