

India Cyber Threat Report 2026: Healthcare, pharma among most targeted

India's healthcare and pharma sectors were heavily targeted by cyberattacks in 2025. Millions of endpoints detected threats, with Trojans and file infectors being the primary culprits.

These attacks risked compromising vital R&D and clinical trial data. Ransomware also caused significant disruption.

In 2025, India's healthcare and pharmaceuticals sector emerged as one of the most heavily targeted industries for cyberattacks, according to the India Cyber Threat Report 2026.

Based on telemetry from more than 8 million endpoints, the report found that education, healthcare and manufacturing together accounted for nearly 47% of all detections between October 2024 and September 2025. Healthcare and pharmaceuticals alone recorded 3.79 million detections, accounting for a 14.24% share.

Based on telemetry from more than 8 million endpoints, the report found that education, healthcare and manufacturing together accounted for nearly 47% of all detections between October 2024 and September 2025. Healthcare and pharmaceuticals alone recorded 3.79 million detections, accounting for a 14.24% share.

The report said Trojans and file infectors made up nearly 70% of all attacks. It also linked remote access Trojans and loader-based malware to attempts to compromise pharmaceutical R&D data and clinical trial information, pointing to espionage and intellectual property theft risks.

Ransomware accounted for less than 1% of total detections but had a significant operational impact. Detections crossed 0.81 million, peaking in January 2025 with 185 incidents and 113,000 detections. Attack vectors included phishing, cracked software, exposed remote desktop services and supply chain compromise.

The report highlights that healthcare data is especially sensitive because it cannot be reissued like payment credentials. Medical histories, diagnostic reports, prescription records, insurance details and other personal data can be exploited for fraud, extortion and long-term profiling.

The impact of such attacks extends beyond data loss. Disruptions to radiology systems can delay diagnoses, manipulated lab results can affect treatment, and stolen clinical trial data can damage research efforts.

The Digital Personal Data Protection (DPDP) Act, 2023 adds further obligations for healthcare institutions, including hospitals, clinics, diagnostic chains, insurers and health-tech platforms. These organizations are required to ensure lawful processing, explicit consent, purpose limitation and strong safeguards for digital personal data across systems such as admission forms, lab reports, teleconsultation logs and wellness app records.