India Cyber Threat Report 2026 Finds Healthcare and Pharma Among India's Most Targeted Sectors

In Indian hospitals and clinics, every beep of a monitor, every diagnostic image, and every electronic prescription reflects a life in care. But in 2025, those same systems also reflected something far darker: a relentless wave of cyberattacks that turned healthcare networks into high-value targets for data theft, extortion, and disruption. The India Cyber Threat Report 2026 by Seqrite, the enterprise security arm of Quick Heal Technologies Limited, a global provider of cybersecurity solutions, highlights how India's healthcare and pharmaceuticals sector has emerged as one of the most attacked verticals in the country.

The report, prepared meticulously by researchers at Seqrite Labs, India's largest malware analaysis facility, draws from telemetry across more than 8 million endpoints. As per the findings of the report, Education, Healthcare, and Manufacturing together accounted for nearly 47% of all detections between October 2024 and September 2025, underscoring how data-rich, always-on environments are squarely in the crosshairs. Healthcare and Pharmaceuticals alone recorded 3.79 million detections (14.24% share), making it one of the most relentlessly targeted sectors in the country.

The report notes that Trojans and file infectors together formed nearly 70% of all attacks. Seqrite telemetry also linked remote access Trojans and loader-based malware to attempts at compromising pharma R&D data and clinical trial information, signaling clear espionage and IP-theft motives. Ransomware added another layer of risk. While it represented less than 1% of total detections, it had a disproportionate operational impact. Ransomware detections exceeded 0.81 million, peaking in January 2025 with 185 incidents and 113,000 detections. Many of these attacks leveraged phishing, cracked software, exposed remote desktop services, or supply chain vectors, which are the same routes used to infiltrate hospital information systems and disrupt care delivery.

Unlike payment data, which can often be reset or rotated, patient records are permanent. Medical histories, diagnostic reports, prescription records, insurance details, and personally identifiable information cannot simply be "reissued" after a breach. This permanence makes healthcare data extraordinarily valuable on underground markets and in extortion schemes, where stolen records are weaponized for blackmail, fraud, and long-term profiling. For healthcare providers, the stakes are no longer limited to system downtime or regulatory penalties. A compromised

radiology system can delay diagnoses. Manipulated lab results can impact treatment. Exfiltrated clinical trial data can undermine years of research investment. In this environment, protecting data is equivalent to protecting patient safety.

India's Digital Personal Data Protection (DPDP) Act, 2023 fundamentally reshapes how healthcare institutions must treat patient data. As Data Fiduciaries, hospitals, clinics, diagnostic chains, insurers, and health-tech platforms are now obligated to ensure lawful processing, explicit consent, purpose limitation, and robust safeguards for every piece of digital personal data they handle – right from admission forms and lab reports to teleconsultation logs and wellness app records.

In this high-risk, high-regulation environment, Seqrite's enterprise security products and allied services emerge not as an optional add-on but as a foundational layer for resilient healthcare operations. Built to address India's evolving threat and compliance realities, all Seqrite products are fully compliant with the provisions of the DPDP Act, ensuring that healthcare organizations can align their cybersecurity investments with India's landmark data protection framework without sacrificing usability or clinical efficiency.