

**Codec Networks**
Coding Threats. Decoding Solutions.

HEALTHCARE & HEALTHTECH CYBERSECURITY

# Safe data. Safe care. Every day.

Patient data protection, hospital application VAPT, SOC, ransomware readiness and medical IoT security for healthcare and healthtech.

## Three questions every healthcare leader should be able to answer

**Could ransomware stop our OPD and labs?**
Segmentation, protected backups and practised downtime procedures decide how long care is disrupted.

**Who can see each patient's records?**
Access to EMR, reports and images should be role-based, logged and reviewed.

**Could we report an incident within six hours?**
CERT-In requires reporting within six hours of noticing an incident; patients and partners expect prompt notice.

**Nov 2022**
AIIMS New Delhi ransomware disruption

**6 hours**
Incident reporting to CERT-In

**180 days**
ICT log retention in India

**May 2027**
Most DPDP obligations take effect

## Built for every healthcare organisation

Hospital chains · standalone hospitals and clinics · diagnostic and imaging networks · telemedicine providers · digital health platforms and health apps · government health programmes.

## The rules that drive your security calendar

| Instrument | Key cybersecurity expectations |
|---|---|
| **DPDP Act & Rules** (2023, 2025) | Patient data safeguards; breach intimation from May 2027 |
| **ABDM · Telemedicine Guidelines** | Consent-based data exchange; teleconsultation privacy and records |
| **CERT-In · CDSCO** | 6-hour reporting, 180-day logs; medical device and software rules |

WHAT WE DO

# Patient data, hospital VAPT, SOC, ransomware readiness and medical IoT

### Patient Data Protection
Health data inventory, EMR access controls, DLP and consent controls.

### Hospital Application VAPT
HIS, EMR, LIS, PACS, portals, apps and health APIs.

### 24/7 SOC
Managed SOC for clinical and IT systems with 6-hour reporting support.

### Ransomware Readiness
Segmentation, immutable backups, downtime procedures and drills.

### Medical IoT Security
Device inventory, testing, segmentation and vendor assessments.

### Privacy & DPDPA
DPDPA readiness, notice and consent, breach workflows.

## Choose your starting point

### Foundation
Network and HIS VAPT, ransomware readiness check, DPDPA quick assessment, phishing awareness. For clinics and standalone hospitals.

### Assurance
Portal, app and API testing, patient data protection, cloud and vendor reviews, managed SOC. For diagnostic networks and healthtech.

### Continuous Resilience
Continuous testing and red teaming, medical IoT programme, SOC with clinical signals, Board reporting. For hospital chains and large platforms.

## Why Codec Networks

### CERT-In empanelled
for information security auditing services, and empanelled with NICSI for application audit services.

### Certified
ISO 9001:2015, ISO/IEC 27001:2022 and ISO/IEC 20000-1:2018.

### Regulation-mapped
Every finding mapped to DPDP, ABDM, CERT-In, telemedicine and device requirements.

### One connected partner
Testing, audits, SOC, forensics and privacy linked from finding to closure.

## Book a scoping session

Share your facilities, systems and partners. We will propose a practical, care-safe assessment and assurance plan.

**New Delhi:** 507, 5th Floor, New Delhi House, Barakhamba Road, Connaught Place – 110001
**Gurugram:** 707, 7th Floor, Silverton Tower, Golf Course Extension Road, Sector 50 – 122018
**Call:** 011 430 496 96 · +91 99716 76124 · +91 88007 88220
**Email:** mktg@codecnetworks.com · www.codecnetworks.com

Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities. Services support risk reduction and assurance and do not guarantee prevention of all incidents or regulatory compliance. Sources: public reporting, CERT-In, MeitY. Confirm obligations against the official instruments.