



Codec Networks

Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · HEALTHCARE & HEALTHTECH

Protect Every Patient. Keep Care Running.

Patient data protection, hospital application VAPT, SOC, ransomware readiness and medical IoT security for hospital chains, diagnostic networks, telemedicine providers and digital health platforms.

Patient Data Protection

Hospital Application VAPT

24/7 SOC

Ransomware Readiness

Medical IoT Security

Privacy & DPDPA

Coding Threats. Decoding Solutions.

www.codecnetworks.com

THE CHALLENGE

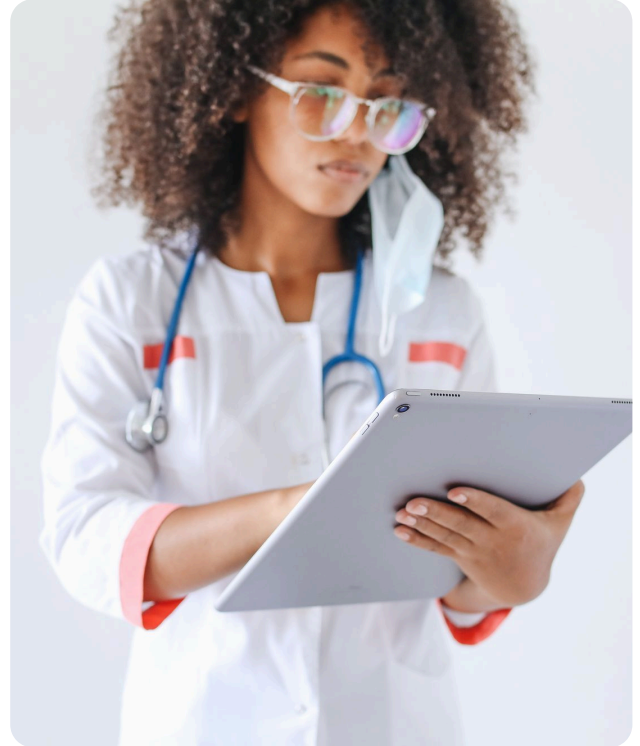
Care depends on your systems. Attackers depend on that.

Hospitals, labs and health platforms hold the most sensitive personal data and run systems that patient care cannot do without.

Ransomware attacks on hospitals—including the 2022 attack on AIIMS New Delhi—show how quickly care can stop.

What keeps leadership teams awake

- Ransomware shutting down HIS, labs and imaging
- Leakage of medical records and reports
- Vulnerable connected medical devices
- Patient apps and portals exposing data
- Vendors and partners with access to clinical systems
- DPDP, ABDM, CERT-In and accreditation obligations



Nov 2022

Ransomware attack disrupted AIIMS New Delhi systems

6 hours

To report cyber incidents to CERT-In

180 days

ICT logs to be kept in India

May 2027

Most DPDP obligations take effect

The rulebook has changed

Instrument	What it means for you
DPDP Act & Rules (2023, 2025)	Lawful processing, safeguards and breach intimation for patient personal data; most obligations from May 2027
ABDM framework and Telemedicine Guidelines	Consent-based health data exchange under ABDM; privacy and record expectations for teleconsultation
CERT-In Directions (28 Apr 2022)	6-hour incident reporting and 180-day logs for all body corporates, including hospitals and health platforms
Device and accreditation requirements	CDSCO rules for medical devices and software; accreditation standards for information management

One partner across the patient journey

Built around our primary proposition for the sector: **patient data protection, hospital application VAPT, SOC, ransomware readiness and medical IoT security.**

Patient Data Protection

- Health data inventory and classification
- Access controls for EMR and records
- DLP for reports and images
- Consent and sharing controls

Hospital Application VAPT

- HIS, EMR, LIS and PACS testing
- Patient portals and mobile apps
- Health APIs and integrations
- Retest and closure tracking

24/7 SOC

- Managed SOC with SIEM and EDR/XDR
- Clinical and IT system monitoring
- Threat hunting
- 6-hour CERT-In reporting support

Ransomware Readiness

- Network segmentation reviews
- Immutable backup and recovery tests
- Downtime procedure reviews
- Ransomware tabletop drills

Medical IoT Security

- Connected device inventory
- Device and management server testing
- IoMT network segmentation
- Device vendor assessments

Privacy & DPDPA

- DPDPA readiness for health data
- Notice and consent reviews
- Breach response workflow
- Third-party data sharing reviews

Who we serve: hospital chains · standalone hospitals and clinics · diagnostic and imaging networks · telemedicine providers · digital health platforms and health apps · government health programmes.

Packaged for how healthcare buys

Eleven Codec Networks bundles apply directly to hospitals, diagnostics and healthtech organisations:

B1

Cyber Assessment & VAPT Assurance

B2

Application, API & DevSecOps Security

B3

Cloud, Infrastructure & Zero Trust

B4

Regulatory Cyber Audit & Compliance

B5

GRC, ISO, SOC 2 & PCI DSS Maturity

B6

Data Privacy & DPDPA Program

B7

Managed SOC, MDR & Threat Monitoring

B8

Forensics, Incident Response & Malware RCA

B9

Third-Party & Supply-Chain Risk

B10

Cyber Simulation, Awareness & Tabletop

B11

Emerging Tech, AI & Web3 Security

Foundation

Clinics and standalone hospitals

- Network and HIS VAPT
- Ransomware readiness check
- Policy and DPDPA quick assessment
- Staff phishing awareness

Assurance

Diagnostic networks and healthtech

- Portal, app and API testing
- Patient data protection programme
- Cloud and vendor reviews
- 24x7 managed SOC

Continuous Resilience

Hospital chains and large platforms

- Continuous testing and red teaming
- Medical IoT security programme
- SOC with clinical-system signals
- Board and accreditation reporting

Mapped to your obligations

Requirement	How we help	Bundle
Patient personal data safeguards and breach intimation (DPDP Act and Rules)	DPDPA programme for health data	B6
Cyber incidents to CERT-In within six hours; 180-day logs	SOC monitoring, IR retainer and reporting support	B7, B8
Consent-based health data exchange (ABDM framework)	Consent-flow and integration testing	B2, B4
Teleconsultation privacy and records (Telemedicine Practice Guidelines)	Telemedicine app and platform testing	B2
Safety and security of medical devices and software (CDSCO)	Medical IoT and device security assessments	B1, B11
Vendor and partner access to patient data	Third-party risk programme	B9
Continuity of clinical services	Ransomware readiness and DR testing	B10, B3

Why healthcare organisations choose Codec Networks

CERT-In empanelled

Independent audits and testing recognised by regulators and partners.

Certified and accountable

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

Clinical-aware testing

HIS, PACS, devices and portals tested without disrupting care.

Ransomware readiness

Segmentation, backups and downtime procedures tested end to end.

Full stack, one partner

Testing, SOC, forensics and privacy connected from finding to closure.

Certified experts

CISA, ISO 27001 LA/LI, CEH, OSCP and CHFI professionals.

How we engage

Discover & scope

Facilities and services, clinical systems and devices, apps and integrations, partners and your audit calendar.

Assess & test

Threat-led testing and regulatory audits executed by certified specialists.

Report in business terms

Findings, risk ratings and a compliance gap matrix for the Board and regulators.

Remediate

Practical, prioritised fixes with technology and compliance teams.

Validate & prove

Retesting and an evidence tracker for auditors, regulators and partners.

Monitor & improve

Managed SOC, recurring testing and quarterly governance reviews.

What you receive: executive summary for the Board or its committee · technical findings with evidence and CVSS ratings · compliance gap matrix · prioritised remediation roadmap · retest reports · audit evidence tracker · SOC dashboards and MTTD/MTTR metrics.



START WITH A SCOPING SESSION

Let's make your next audit, upgrade and incident a non-event.

Tell us 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, New Delhi – 110001

Gurugram

707, 7th Floor, Silverton Tower, Golf Course Extension Road, Sector 50, Gurugram – 122018, Haryana

Call

011 430 496 96 · 011 437 522 99
+91 99716 76124 · +91 88007 88220 · +91 88003 31124

Write

mktg@codecnetworks.com
www.codecnetworks.com

Codec Networks

Coding Threats. Decoding Solutions.

Secure Today. Innovate Tomorrow. Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities. Packages are proposed groupings of Codec Networks bundles, finalised through scoping. 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.