Codec Networks

Coding Threats. Decoding Solutions.

HEALTHCARE & HEALTHTECH

Protect Every Patient. Keep Care Running.

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



What we will cover

The sector and its risks

Scale, players and the threats that matter most

What regulators now expect

DPDP, ABDM, Telemedicine Guidelines, CERT-In and CDSCO

How Codec Networks helps

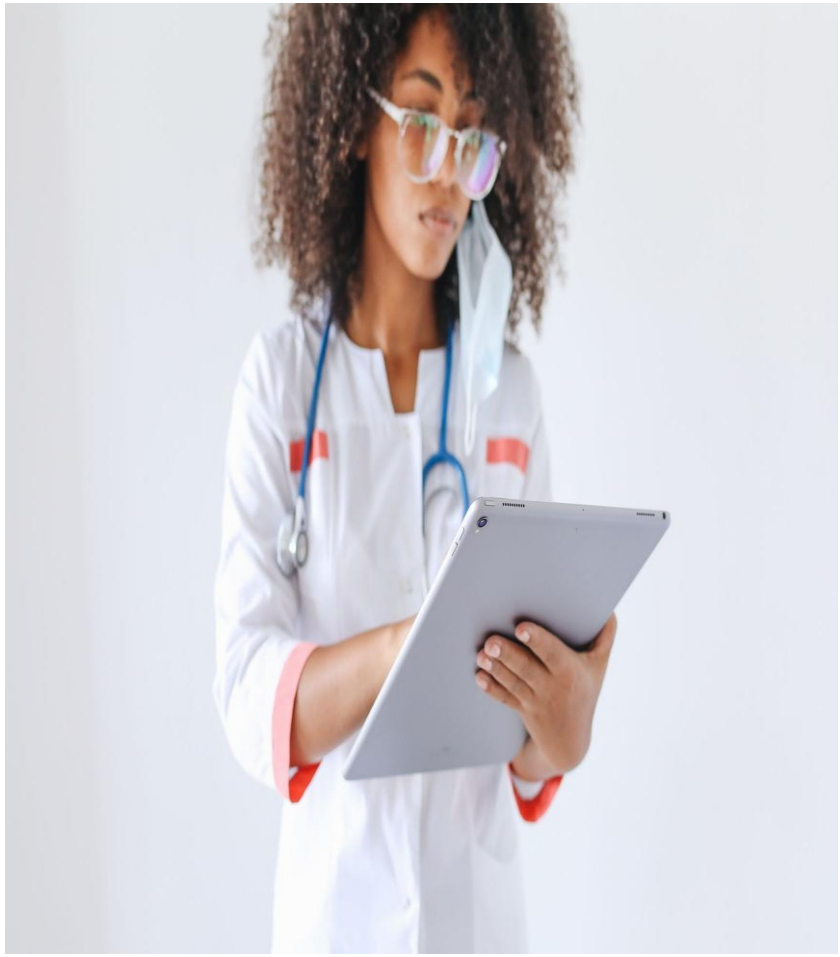
Services, bundles and packages built for the sector

Proof in scenarios

Five new case studies and the controls that break the chain

Why Codec Networks and next steps

Our value add and how to start



Healthcare is a top ransomware target

Downtime affects patients, not just data

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

What this means: healthcare organisations must protect patient data, keep clinical systems running through ransomware, secure connected devices and apps, manage consent-based sharing and report incidents within six hours.

Sources: public reporting, CERT-In, MeitY, NHA.

Who we serve across healthcare and healthtech

Hospital chains

Multi-specialty networks

Standalone hospitals

Nursing homes and clinics

Diagnostic networks

Labs and imaging

Telemedicine

Remote consultations

Digital health platforms

Records and care apps

Pharmacy platforms

Online and retail pharmacy

Government health programmes

Public schemes

Health insurers and TPAs

Claims partners

The threats that cost healthcare the most

Six priorities from our 18-threat healthcare assessment

Ransomware

OPD, labs and imaging stop

Patient data leakage

Records and reports exposed

Medical IoT attacks

Devices on flat networks

Portal and API exposure

Reports for anyone who asks

Vendor compromise

Partners with clinical access

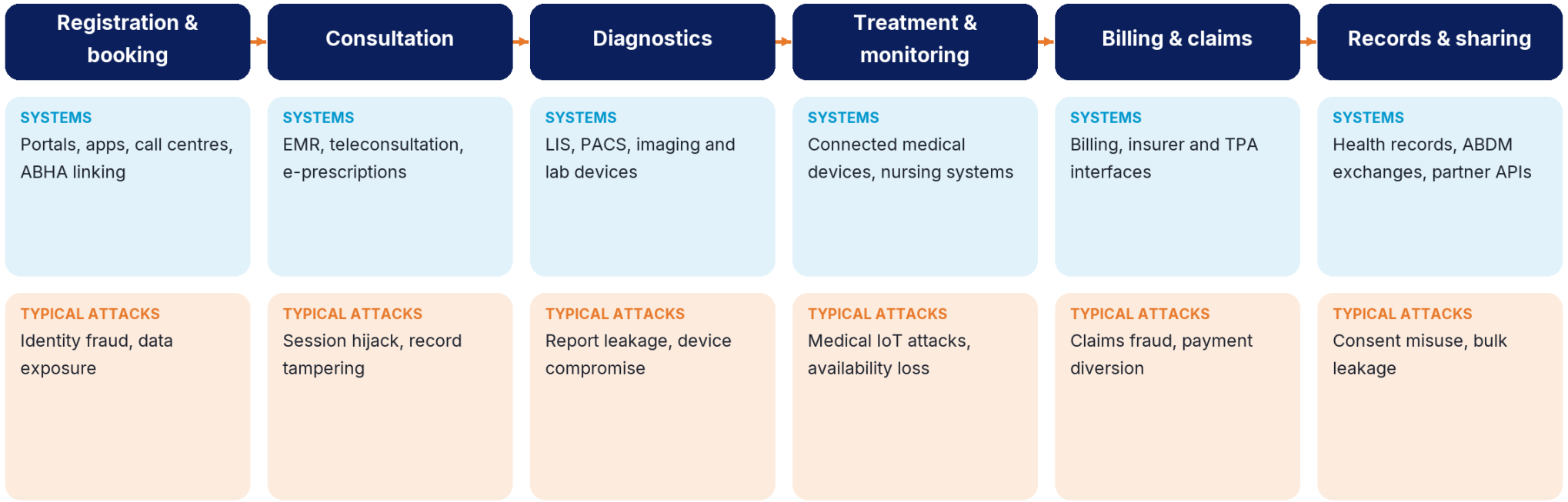
Slow detection & reporting

Missing the 6-hour window

Attacks target every step of the patient journey

Where Cyber Risk Sits in the Patient Journey

Every step from registration to billing carries its own attack surface



Hospitals must protect both patient data and the availability of systems that care depends on.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

DPDP, ABDM, Telemedicine Guidelines, CERT-In and CDSCO

Codec Networks
Coding Threats. Decoding Solutions.

The rules that shape healthcare cybersecurity

Requirement	Frequency / deadline	Source
Patient personal data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
Sensitive personal data (until replaced by DPDP)	In force	IT (SPDI) Rules, 2011
Consent-based health data exchange	Per ABDM framework	NHA / ABDM
Teleconsultation practice	In force since Mar 2020	Telemedicine Practice Guidelines
Cyber incident reporting	To CERT-In within 6 hours	CERT-In Directions, 2022
ICT log retention	180 days, in India	CERT-In Directions, 2022
Medical devices and software	Per device class	Medical Devices Rules, 2017 (CDSCO)
Records at clinical establishments	Per state adoption	Clinical Establishments Act, 2010

Key dates on the regulatory timeline

Regulatory Timeline for Healthcare Cybersecurity

Key health-sector and cross-sector instruments shaping healthcare cybersecurity

In force Upcoming (from Oct 2026)

2011	IT (SPDI) Rules classify medical records as sensitive personal data
Mar 2020	Telemedicine Practice Guidelines issued
Sep 2021	Ayushman Bharat Digital Mission launched nationally
Apr 2022	CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Aug 2023	Digital Personal Data Protection Act, 2023 enacted
Nov 2025	DPDP Rules, 2025 notified with phased commencement
May 2027	**Most DPDP Rules obligations, incl. breach intimation, take effect**

Sources: MeitY, MoHFW, NHA, CERT-In. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

Patient data · Hospital VAPT · SOC · Ransomware readiness · Medical IoT · Privacy

Codec Networks
Coding Threats. Decoding Solutions.

One partner across the patient journey



Patient Data Protection

Inventory, EMR access, DLP, consent



Hospital Application VAPT

HIS, EMR, LIS, PACS, portals, APIs



24/7 SOC

Clinical and IT monitoring



Ransomware Readiness

Segmentation, backups, downtime drills



Medical IoT Security

Devices, servers, segmentation



Privacy & DPDPA

Notice, consent, breach workflow

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services

- **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

Bundle numbers follow the Codec Networks Bundled Service Models. Scope, frequency and pricing are confirmed during scoping.

Three packages, sized to where you are

Foundation

Clinics and standalone hospitals

- Network and HIS VAPT (B1)
- Ransomware readiness check (B10)
- DPDPA quick assessment (B6)
- Phishing awareness (B10)

Assurance

Diagnostic networks and healthtech

- Portal, app and API testing (B2)
- Patient data protection (B6)
- Cloud and vendor reviews (B3, B9)
- 24x7 managed SOC (B7)

Continuous Resilience

Hospital chains and large platforms

- Red teaming and simulations (B1, B10)
- Medical IoT programme (B1, B3)
- SOC with clinical signals (B7)
- Board and accreditation reporting (B5)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	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

Five new case studies, five broken chains

Illustrative composite scenarios written for 2026—not client engagements

1	**The Ransomware That Closed the OPD**	Ransomware stops HIS, labs and PACS; segmentation and backups limit it	B7 · B10 · B8
2	**The Lab Report Portal That Listed Everyone**	Sequential report links leak results; access testing prevents it	B2 · B6 · B7
3	**The Teleconsult App That Logged Too Much**	SDKs share symptoms with ad platforms; app privacy testing prevents it	B2 · B6 · B9
4	**The Infusion Pumps on the Guest Wi-Fi**	Malware disrupts devices on a flat network; IoMT segmentation prevents it	B3 · B1 · B7
5	**The Health Records Pulled Without Consent**	An integration skips consent checks; consent-flow testing prevents it	B2 · B6 · B4

Example: breaking a hospital ransomware chain

Case 1: The Ransomware That Closed the OPD

ILLUSTRATIVE ATTACK PATH

Step 1
A phishing email compromises a billing workstation

→

Step 2
Attacker spreads through a flat hospital network

→

Step 3
HIS, LIS and PACS servers are encrypted

→

Step 4
Registration, labs and imaging stop; staff revert to paper

→

Step 5
Patients diverted; CERT-In reporting and recovery

WHERE CONTROLS BREAK THE CHAIN

- Segmentation of clinical, admin and device networks
- 24x7 SOC with EDR on servers
- Immutable backups and tested recovery
- Downtime procedures and ransomware drills

Illustrative composite scenario prepared by Codec Networks. Not a client engagement.

Codec Networks

What we test: phishing resilience, segmentation between admin, clinical and device networks, EDR and 24x7 monitoring, immutable backups and restore times for HIS, LIS and PACS, downtime procedures and the CERT-In reporting step.

Why healthcare organisations choose Codec Networks

CERT-In empanelled

For information security auditing services; NICSI empanelled for application audits

Certified

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

Regulation-mapped

Mapped to DPDP, ABDM, CERT-In, telemedicine and device requirements

Tests the whole chain

Technical, process and monitoring tests together

Full stack, one partner

VAPT, audits, SOC, forensics, privacy and Board advisory connected

Specialist experts

CEH, OSCP, CPENT, CISA, ISO 27001 LA/LI, CHFI; OWASP, MITRE ATT&CK, NIST



How we deliver, and what you receive

Codec Networks Delivery Methodology

Nine stages, from scoping to continuous improvement



Source: Codec Networks project and service delivery methodology

Codec Networks

- Executive summary for the Board or its committee
- Technical findings with evidence and CVSS ratings
- Compliance gap matrix mapped to your obligations
- Prioritised remediation roadmap and retest reports
- Audit evidence tracker for regulators and partners
- SOC dashboards with MTTD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Facilities, clinical systems, devices, apps, partners and audit calendar

2 Proposal

Regulation-mapped scope, methodology, timeline and deliverables

3 Kick-off

Testing, audit or SOC onboarding, with Board-ready reporting

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

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

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.

Codec Networks
Coding Threats. Decoding Solutions.