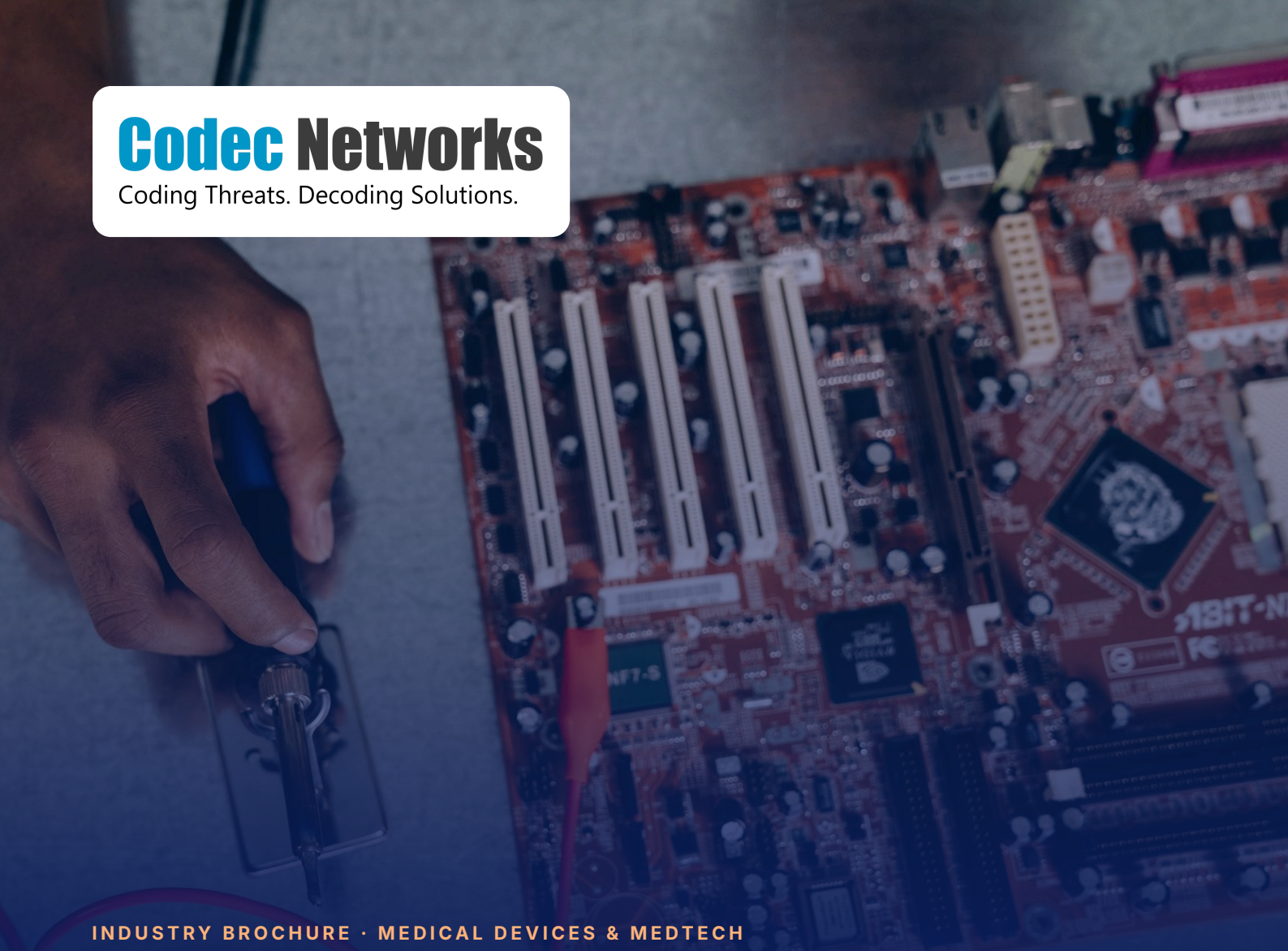


Codec Networks
Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · MEDICAL DEVICES & MEDTECH

Secure by Design. Safe in Every Hand.

Embedded and firmware testing, device and API security, secure updates and product threat modelling for connected device manufacturers, diagnostic equipment vendors and remote monitoring platforms.

- Embedded & Firmware Testing
- Device & API Security
- Secure Updates
- Product Threat Modelling
- SBOM & Vulnerability Management
- Regulatory Evidence

THE CHALLENGE

Your device ships once. Its security must last for years.

Connected medical devices carry firmware, wireless interfaces, apps and cloud links into hospitals and homes. Export regulators now require cybersecurity evidence in submissions, and CDSCO's medical device software guidance addresses cybersecurity in India.



What keeps leadership teams awake

- Firmware vulnerabilities and hard-coded credentials
- Unsigned updates and compromised update servers
- Exposed debug ports and extractable keys
- Insecure wireless, apps and cloud APIs
- Vulnerable third-party components without an SBOM
- FDA 524B, EU MDR and CDSCO evidence for approvals

Mar 2023
US FDA cyber-device requirements (section 524B) in effect

Oct 2023
Licensing phased in for all device classes in India

6 hours
To report cyber incidents to CERT-In

May 2027
Most DPDP obligations take effect

The rulebook has changed

Instrument	What it means for you
Medical Devices Rules, 2017 and CDSCO software guidance	Risk-based licensing of devices; guidance for medical device software addressing cybersecurity (finalised 2026, as reported)
US FDA section 524B (Mar 2023)	Cyber devices need a cybersecurity plan, SBOM, vulnerability management and design controls in premarket submissions
EU MDR and standards	General safety requirements covering IT security; MDCG guidance; IEC 81001-5-1, IEC 62304 and ISO 14971
CERT-In Directions · DPDP Act & Rules	6-hour incident reporting for platforms; patient data safeguards from May 2027

OUR SERVICE OFFERINGS

One partner from circuit board to cloud

Built around our primary proposition for the sector: **embedded and firmware testing, device and API security, secure updates and product threat modelling.**

Embedded & Firmware Testing

- Firmware extraction and analysis
- Hard-coded secret and backdoor detection
- Debug port and hardware testing
- RTOS and bootloader review

Device & API Security

- BLE, Wi-Fi and cellular testing
- Device-to-cloud API testing
- Mobile companion app testing
- Authentication and pairing reviews

Secure Updates

- Firmware signing and verified boot
- Update server hardening
- Rollback and staged rollout design
- Service tool security

Product Threat Modelling

- Threat models aligned to ISO 14971
- Security risk assessments
- Security requirements and architecture
- Traceability for submissions

SBOM & Vulnerability Management

- SBOM generation and analysis
- Third-party component risk
- Coordinated vulnerability disclosure
- Post-market monitoring

Regulatory Evidence

- FDA 524B submission evidence
- EU MDR cybersecurity documentation
- CDSCO software guidance alignment
- IEC 81001-5-1 lifecycle readiness

Who we serve: connected device manufacturers · diagnostic and imaging equipment vendors · wearable and home-care device makers · software-as-a-medical-device developers · remote monitoring and IoMT platform providers.

BUNDLED SERVICE MODELS

Packaged for how medtech companies buy

Eleven Codec Networks bundles apply directly to medical device and medtech companies:

- **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

Start-ups and first-product teams

- Product threat model
- Firmware and app security test
- SBOM generation
- Submission evidence checklist

Assurance

Growing manufacturers

- Full device, API and cloud testing
- Secure update review
- IEC 81001-5-1 gap assessment
- Vulnerability disclosure programme

Continuous Resilience

Established OEMs and platforms

- Continuous product security testing
- Supplier and component assurance
- Fleet and platform monitoring
- Post-market and Board reporting

Mapped to your obligations

Requirement	How we help	Bundle
Device licensing and quality (Medical Devices Rules, 2017)	Security evidence supporting quality documentation	B4
Cybersecurity of medical device software (CDSCO guidance)	Software security assessment and documentation	B2, B4
Cybersecurity plan, SBOM and design controls for cyber devices (US FDA 524B)	Threat modelling, SBOM and penetration testing evidence	B1, B2, B4
IT security in general safety requirements (EU MDR)	Cybersecurity documentation and testing	B4
Secure product lifecycle (IEC 81001-5-1)	Lifecycle gap assessment and implementation	B5
Patient data safeguards for platforms (DPDP)	DPDPA programme for device data	B6
Cyber incidents to CERT-In within six hours (platforms)	Platform monitoring and IR support	B7, B8

THE CODEC NETWORKS VALUE ADD

Why medtech companies choose Codec Networks

CERT-In empanelled

Independent testing recognised by regulators, hospitals and partners.

Certified and accountable

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

Hardware to cloud

Firmware, wireless, apps and cloud platforms tested together.

Submission-ready evidence

Threat models, SBOMs and test reports structured for regulators.

Full stack, one partner

Product testing, platform SOC, forensics and privacy connected.

Certified experts

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

How we engage

Discover & scope

Device architecture, connectivity, software and cloud, target markets and your submission 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 submission, release and field incident a non-event.

Tell us your devices, platforms and target markets. We will propose a practical product security and evidence 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: US FDA, CDSCO, CERT-In, MeitY. Confirm requirements against the official texts.