Codec Networks

Coding Threats. Decoding Solutions.

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 medical device and medtech companies

What we will cover

The sector and its risks

Scale, players and the threats that matter most

What regulators now expect

Medical Devices Rules, CDSCO software guidance, FDA 524B, EU MDR and standards

How Codec Networks helps

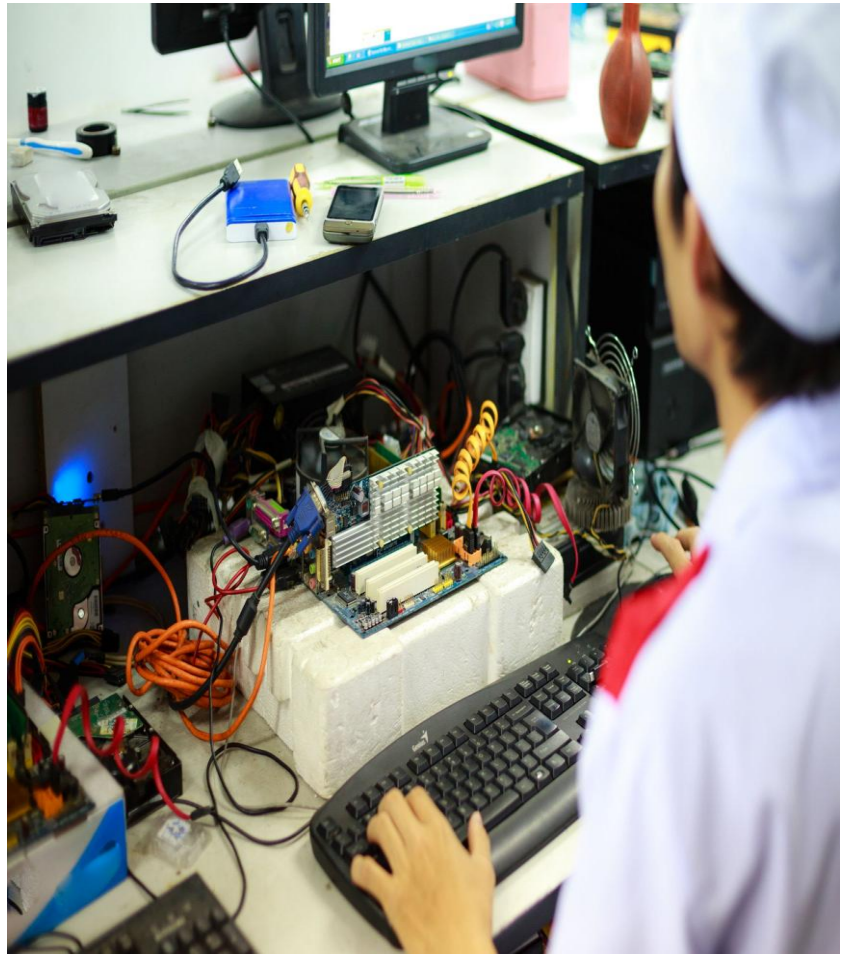
Services, bundles and packages built for the sector

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



Device cybersecurity is now an approval requirement

Regulators ask for threat models, SBOMs and test evidence

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

What this means: medtech companies must design security in, test firmware, wireless, apps and cloud, maintain SBOMs and secure updates, handle vulnerabilities for the life of the device and produce evidence for regulators.

Sources: US FDA, CDSCO, CERT-In, MeitY.

Who we serve across medical devices and medtech

Bedside device makers

Monitors, pumps, ventilators

Imaging and lab equipment

Scanners and analysers

Wearables and home devices

Consumer-grade medical devices

Implantables

Implanted and life-sustaining devices

SaMD developers

Software as a medical device

Remote monitoring platforms

IoMT cloud and apps

Contract manufacturers

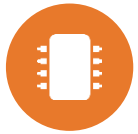
Device and board assembly

Service and distribution

Field service partners

The threats that cost medtech companies the most

Six priorities from our 18-threat medtech assessment



Firmware vulnerabilities

Flaws in every shipped unit

Hard-coded credentials

Backdoors in components

Insecure updates

Fake firmware for the fleet

Wireless and app flaws

BLE, Wi-Fi and companion apps

Cloud platform exposure

Patient data at scale

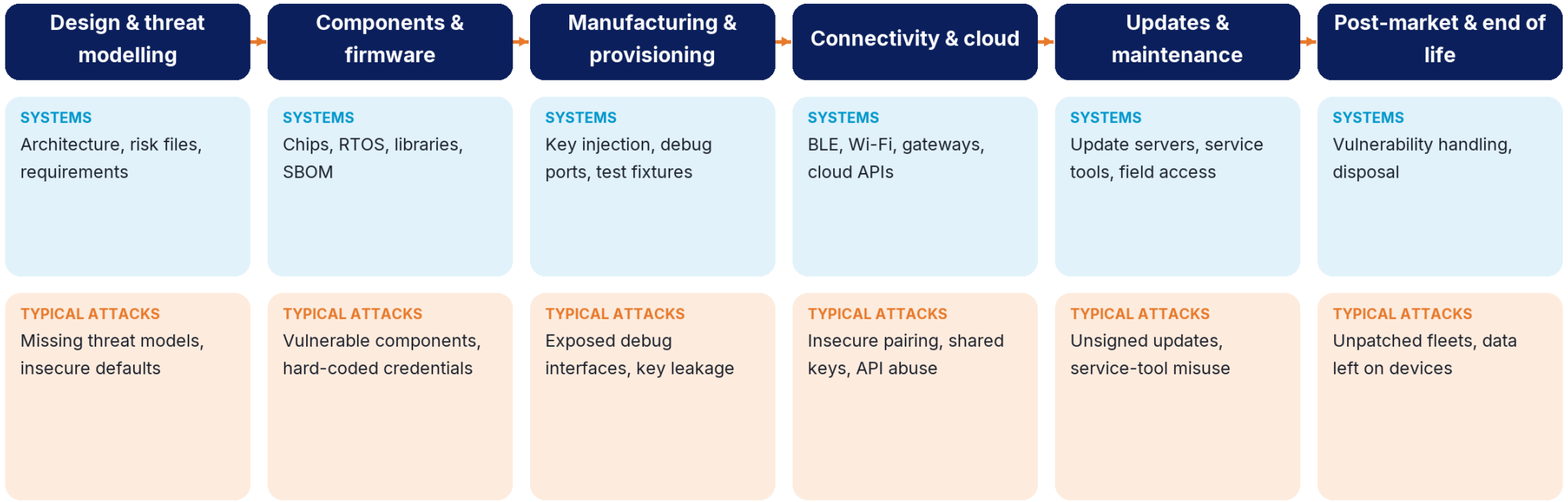
Weak vulnerability handling

Slow fixes across the fleet

Attacks target every stage of the device lifecycle

Where Cyber Risk Sits in the Device Lifecycle

Every stage from design to decommissioning carries its own attack surface



Device security must be designed in, tested before release and maintained for the life of every unit in the field.

Source: Codec Networks analysis

Codec Networks

Codec Networks
Coding Threats. Decoding Solutions.

What regulators now expect

Medical Devices Rules, CDSCO software guidance, FDA 524B, EU MDR and standards

Codec Networks
Coding Threats. Decoding Solutions.

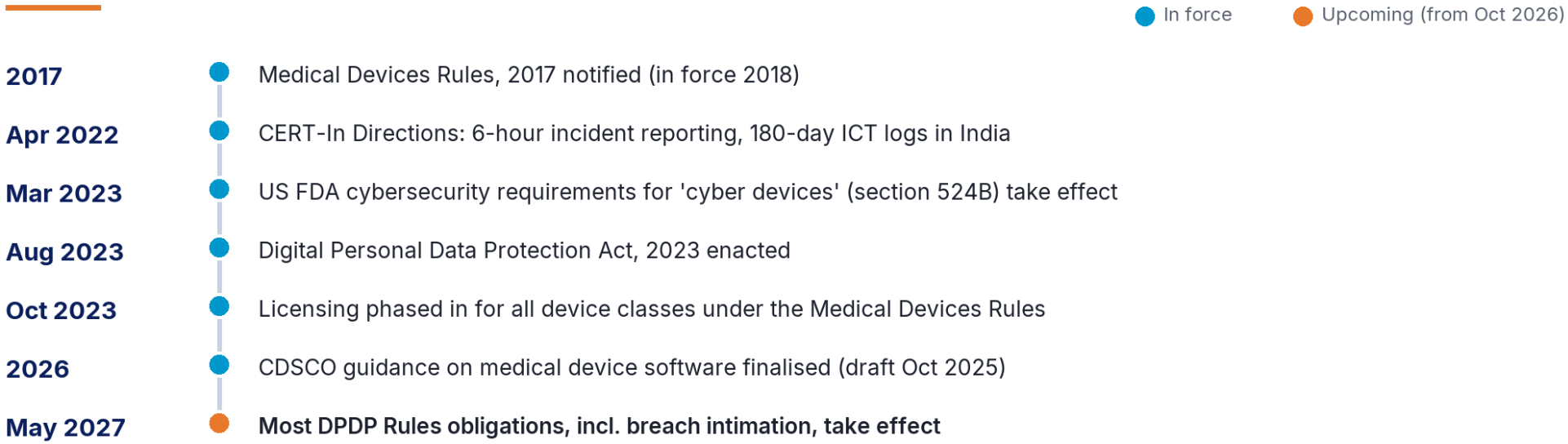
The rules and standards shaping device security

Requirement	Frequency / deadline	Source
Device licensing in India	All classes since Oct 2023	Medical Devices Rules, 2017
Medical device software	Guidance finalised 2026 (as reported)	CDSCO MDSW guidance
Cyber devices in the US	In effect since Mar 2023	FD&C Act section 524B
Devices in the EU	In force	EU MDR 2017/745; MDCG guidance
Secure product lifecycle	Standard	IEC 81001-5-1
Software lifecycle and risk	Standards	IEC 62304; ISO 14971
Platform incident reporting	To CERT-In within 6 hours	CERT-In Directions, 2022
Patient data from devices	Most obligations from May 2027	DPDP Act 2023 and Rules 2025

Key dates on the regulatory timeline

Regulatory Timeline for Medical Device Cybersecurity

Key Indian and export-market instruments shaping device security



Sources: CDSCO, US FDA, CERT-In, MeitY. Confirm requirements against the official texts.

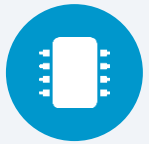
Codec Networks

How Codec Networks helps

Firmware · Device & API · Secure updates · Threat modelling · SBOM · Regulatory evidence

Codec Networks
Coding Threats. Decoding Solutions.

One partner from circuit board to cloud



Embedded & Firmware Testing

Firmware, secrets, debug ports

Device & API Security

Wireless, apps, cloud APIs

Secure Updates

Signing, verified boot, update servers

Product Threat Modelling

Threat models and risk files

SBOM & Vulnerability Management

Components, disclosure, post-market

Regulatory Evidence

FDA 524B, EU MDR, CDSCO

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

Start-ups and first-product teams

- Product threat model (B2)
- Firmware and app test (B1)
- SBOM generation (B2)
- Submission checklist (B4)

Assurance

Growing manufacturers

- Device, API and cloud testing (B1, B3)
- Secure update review (B2)
- IEC 81001-5-1 gap assessment (B5)
- Disclosure programme (B5)

Continuous Resilience

Established OEMs and platforms

- Continuous product testing (B1, B10)
- Supplier assurance (B9)
- Fleet and platform monitoring (B7)
- Post-market reporting (B4)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	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

Five new case studies, five broken chains

Illustrative composite scenarios written for 2026—not client engagements

1	**The Monitor That Phoned Home**	A component hides a remote connection; SBOM and firmware analysis find it	**B1 · B9 · B4**
2	**The Update Server That Shipped Malware**	A tampered update reaches the fleet; signing and verified boot stop it	**B2 · B3 · B8**
3	**The Debug Port on the Production Board**	Open debug ports leak shared keys; hardware testing prevents it	**B1 · B2 · B5**
4	**The Remote Monitoring Cloud With One Key**	A shared API key exposes patient data; per-device identity prevents it	**B2 · B3 · B6**
5	**The Export Submission That Came Back**	Thin cyber documentation delays approval; threat models and SBOMs fix it	**B4 · B2 · B5**

Example: breaking a malicious-update chain

Case 2: The Update Server That Shipped Malware

ILLUSTRATIVE ATTACK PATH

Step 1
A device maker's update server is poorly protected

→

Step 2
Attacker uploads a tampered firmware image

→

Step 3
Devices accept the update without signature checks

→

Step 4
Field units malfunction or are compromised

→

Step 5
Recall-scale response and regulator notifications

WHERE CONTROLS BREAK THE CHAIN

- Cryptographically signed firmware with verified boot
- Hardened, monitored update infrastructure
- Staged rollouts and rollback
- Product incident response plan

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

Codec Networks

What we test: firmware signing and verification on the device, verified boot, update server hardening and monitoring, staged rollout and rollback, and the product incident and regulator notification steps.

Why medtech companies 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 CDSCO, FDA 524B, EU MDR, IEC 81001-5-1, CERT-In and DPDP

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

Device architecture, connectivity, cloud, target markets and submission 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.