

Codec Networks
Coding Threats. Decoding Solutions.

MEDICAL DEVICES & MEDTECH CYBERSECURITY

Secure devices. Approved faster.

Embedded and firmware testing, device and API security, secure updates and product threat modelling for medtech.

Three questions every medtech leader should be able to answer

Do we know every component inside our device?
An SBOM is now expected by regulators and hospitals—and is essential when a component vulnerability is published.

Could someone push a fake update to our fleet?
Signed firmware, verified boot and hardened update servers protect every unit in the field.

Is our submission evidence ready?
Threat models, test reports and vulnerability plans are part of approvals in key export markets.

Mar 2023
FDA cyber-device rules in effect

Oct 2023
All device classes licensed in India

6 hours
Incident reporting to CERT-In

May 2027
Most DPDP obligations take effect

Built for every medtech company

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.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
Medical Devices Rules · CDSCO software guidance	Device licensing; software cybersecurity guidance
US FDA 524B · EU MDR	Cybersecurity plan, SBOM, design controls; IT security requirements
CERT-In · DPDP	6-hour reporting for platforms; patient data safeguards

WHAT WE DO

Firmware testing, device and API security, secure updates and threat modelling

Embedded & Firmware Testing
Firmware analysis, hard-coded secrets, debug ports and bootloaders.

Device & API Security
Wireless, pairing, device-to-cloud APIs and companion apps.

Secure Updates
Signing, verified boot, update servers and service tools.

Product Threat Modelling
Threat models and security risk assessments aligned to ISO 14971.

SBOM & Vulnerability Management
SBOMs, component risk, disclosure and post-market monitoring.

Regulatory Evidence
FDA 524B, EU MDR, CDSCO and IEC 81001-5-1 documentation.

Choose your starting point

Foundation
Product threat model, firmware and app test, SBOM, submission checklist. For start-ups and first-product teams.

Assurance
Device, API and cloud testing, secure update review, IEC 81001-5-1 gap assessment, disclosure programme. For growing manufacturers.

Continuous Resilience
Continuous product testing, supplier assurance, fleet and platform monitoring, post-market reporting. For established OEMs and 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 CDSCO, FDA 524B, EU MDR, IEC 81001-5-1, CERT-In and DPDP.

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

Book a scoping session

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