



Codec Networks

Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · PHARMACEUTICALS & LIFE SCIENCES

Protect the Science. Keep the Plant Running.

Research and IP protection, clinical data privacy, OT security and cloud and vendor assessments for drug manufacturers, biotechnology firms, CROs and clinical research and laboratory businesses.

Research & IP Protection

Clinical Data Privacy

OT Security

Data Integrity

Cloud & Vendor Assessments

24/7 SOC

Coding Threats. Decoding Solutions.

www.codecnetworks.com

THE CHALLENGE

Your molecules and your plants are both targets.

Pharma companies hold valuable research IP, regulated quality data and clinical data, and run plants whose downtime affects patients worldwide. Revised Schedule M, global GMP and data integrity expectations make computerised-system controls a regulatory issue too.

What keeps leadership teams awake

- Ransomware crossing from IT into plant OT
- Theft of formulations and research data
- Data integrity gaps in lab and quality systems
- Clinical trial data leakage at CROs and sites
- Partners and vendors with access to plants and data
- Schedule M, export inspections, CERT-In and DPDP obligations



Dec 2025

Revised Schedule M
deadline for MSME
manufacturers

2019

New Drugs and Clinical
Trials Rules notified

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
Revised Schedule M (GMP) (notified Dec 2023)	Modernised good manufacturing practices, including expectations for quality systems and computerised systems
New Drugs and Clinical Trials Rules, 2019	Clinical trial conduct, records and participant protection, alongside ICMR ethical guidelines
Global GMP and data integrity	US FDA 21 CFR Part 11, EU GMP Annex 11, WHO and PIC/S guidance for export markets
CERT-In Directions · DPDP Act & Rules	6-hour incident reporting, 180-day logs; participant and employee data safeguards from May 2027

One partner from lab bench to plant floor

Built around our primary proposition for the sector: **research and IP protection, clinical data privacy, OT security and cloud and vendor assessments.**

Research & IP Protection

- R&D data classification
- DLP for research assets
- Insider-threat monitoring
- Collaboration platform reviews

Clinical Data Privacy

- EDC, CTMS and trial app testing
- Participant data protection and DPDPA
- CRO and site security assessments
- Breach response workflows

OT Security

- Plant OT asset inventory
- IT/OT segmentation and DMZ review
- MES, SCADA and DCS assessments
- OT monitoring and vendor access

Data Integrity

- Computerised system security reviews
- Audit trail and access controls
- LIMS and CDS configuration reviews
- Inspection-readiness evidence

Cloud & Vendor Assessments

- Cloud and SaaS configuration reviews
- CRO, CDMO and vendor assessments
- Equipment vendor access reviews
- Contract security clauses

24/7 SOC

- Managed SOC for IT and OT
- Espionage-focused threat hunting
- Ransomware detection
- 6-hour CERT-In reporting support

Who we serve: formulation and API manufacturers · biologics and biotechnology firms · contract research organisations · clinical sites and contract laboratories · CDMOs and CMOs · pharma distributors and exporters.

Packaged for how pharma companies buy

Eleven Codec Networks bundles apply directly to pharmaceutical and life sciences 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

MSME manufacturers and labs

- IT and plant network VAPT
- Data integrity quick review
- Policy and ISO 27001 gap check
- Backup and recovery check

Assurance

Mid-sized manufacturers and CROs

- OT segmentation and assessment
- LIMS, EDC and QMS testing
- Clinical data privacy programme
- 24x7 managed SOC

Continuous Resilience

Large pharma and biotech

- Continuous IT/OT testing and red teaming
- IP protection and insider programme
- SOC with OT and espionage signals
- Board and inspection-readiness reporting

Mapped to your obligations

Requirement	How we help	Bundle
Good manufacturing practices including computerised systems (Revised Schedule M)	Computerised system and data integrity assessment	B4
Electronic records and signatures for export markets (21 CFR Part 11, EU Annex 11)	Data integrity and access control review	B4, B5
Clinical trial records and participant protection (NDCT Rules 2019, ICMR guidelines)	Clinical platform testing and privacy programme	B2, B6
Cyber incidents to CERT-In within six hours; 180-day logs	SOC monitoring, IR retainer and reporting support	B7, B8
Participant and employee personal data safeguards (DPDP)	DPDPA programme	B6
Partner and vendor controls (CRO, CDMO and licensing contracts)	Third-party risk programme	B9
Continuity of supply (customer and regulator expectations)	OT resilience and recovery testing	B3, B10

Why pharma companies 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.

IT and OT depth

Plant OT, lab systems and clinical platforms assessed safely.

Data integrity aware

Findings framed for GMP, Part 11 and Annex 11 expectations.

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

Sites and plants, lab and clinical systems, export markets, partners and your inspection 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 MTTR/MTTD metrics.



START WITH A SCOPING SESSION

Let's make your next inspection, batch and incident a non-event.

Tell us your sites, systems and partners. We will propose a practical, GMP-aware 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: CDSCO, MoHFW, CERT-In, MeitY. Confirm obligations against the official notifications.