

Protected science. Resilient supply.

Research and IP protection, clinical data privacy, OT security and cloud and vendor assessments for pharma and life sciences.

Three questions every pharma leader should be able to answer

Could ransomware stop our plants?

IT/OT segmentation, OT monitoring and offline recovery decide whether an IT incident becomes a production stop.

Would we know if research data walked out?

Classification, DLP and behaviour monitoring catch insider and espionage exfiltration.

Would our audit trails survive an inspection?

Unique access, enabled audit trails and regular reviews are both GMP and security controls.

Dec 2025

Schedule M MSME
deadline

2019

NDCT Rules notified

6 hours

Incident reporting to
CERT-In

May 2027

Most DPDP obligations
take effect

Built for every life sciences organisation

Formulation and API manufacturers · biologics and biotechnology firms · contract research organisations · clinical sites and contract laboratories · CDMOs and CMOs · pharma distributors and exporters.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
Revised Schedule M · NDCT Rules (2023, 2019)	GMP including computerised systems; clinical trial records and participant protection
Global GMP and data integrity	21 CFR Part 11, EU Annex 11, WHO and PIC/S guidance
CERT-In · DPDP	6-hour reporting, 180-day logs; participant data safeguards

WHAT WE DO

Research and IP protection, clinical privacy, OT security and vendor assessments

Research & IP Protection

R&D data classification, DLP, insider monitoring and collaboration reviews.

Clinical Data Privacy

EDC and CTMS testing, participant data protection, CRO assessments.

OT Security

Plant OT inventory, IT/OT segmentation, MES and SCADA assessments.

Data Integrity

Computerised system, audit trail and access reviews for LIMS and CDS.

Cloud & Vendor Assessments

Cloud, SaaS, CRO, CDMO and equipment vendor reviews.

24/7 SOC

Managed SOC for IT and OT with espionage-focused hunting.

Choose your starting point

Foundation

IT and plant network VAPT, data integrity quick review, ISO 27001 gap check, backup check. For MSME manufacturers and labs.

Assurance

OT segmentation and assessment, LIMS, EDC and QMS testing, clinical data privacy, managed SOC. For mid-sized manufacturers and CROs.

Continuous Resilience

Continuous IT/OT testing and red teaming, IP protection programme, SOC with OT signals, Board reporting. For large pharma and biotech.

Why Codec Networks

CERT-In empanelled

for information security auditing services, and empanelled with NISCI for application audit services.

Certified

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

Regulation-mapped

Every finding mapped to Schedule M, NDCT Rules, global data integrity, CERT-In and DPDP.

One connected partner

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

Book a scoping session

Share 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 – 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: CDSCO, MoHFW, CERT-In, MeitY. Confirm obligations against the official notifications.