

Codec Networks

Coding Threats. Decoding Solutions.

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 pharma and life sciences

Coding Threats. Decoding Solutions. · www.codecnetworks.com



What we will cover



The sector and its risks

Scale, players and the threats that matter most



What regulators now expect

Revised Schedule M, NDCT Rules, global data integrity, CERT-In and DPDP



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



Quality rules now meet cybersecurity

Schedule M, clinical rules and export inspections all depend on trustworthy systems

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

What this means: pharma organisations must keep plants running through cyber incidents, protect research IP, assure data integrity in lab and quality systems, protect trial participants' data and report incidents within six hours.

Sources: CDSCO, MoHFW, CERT-In, MeitY.

Who we serve across pharma and life sciences



Formulation manufacturers

Generics and branded products



API manufacturers

Active ingredients



Biologics and biotech

Vaccines, biosimilars, research



Contract research organisations

Clinical trial services



Clinical sites and labs

Trials and testing



CDMOs and CMOs

Contract manufacturing



Distributors and exporters

Supply and cold chain



Medical and regulatory affairs

Dossiers and submissions

The threats that cost pharma the most

Six priorities from our 18-threat pharma assessment



Ransomware into OT

Plants and batch release stop



IP theft and espionage

Formulations and research



Data integrity failures

Audit trails and access gaps



Clinical data leakage

Participant health data



Partner compromise

CROs, CDMOs and vendors



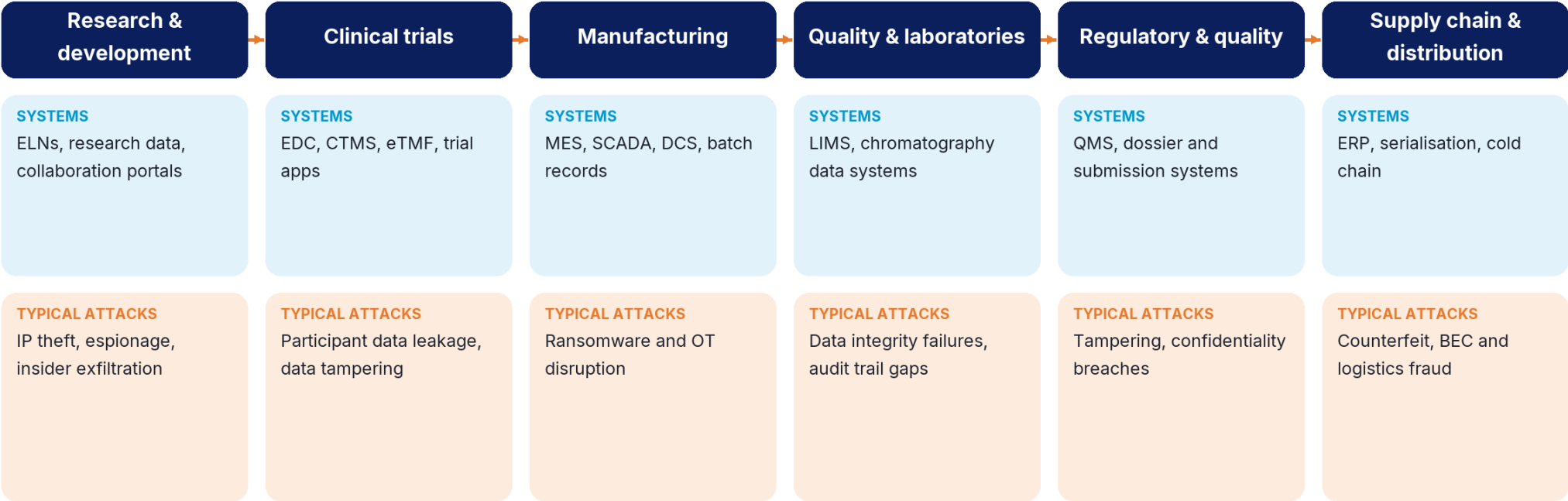
Slow detection & reporting

Missing the 6-hour window

Attacks target every stage from molecule to market

Where Cyber Risk Sits in the Pharma Value Chain

Every stage from molecule to market carries its own attack surface



Data integrity is a regulatory requirement as well as a security outcome—what attackers change, inspectors will find.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

Revised Schedule M, NDCT Rules, global data integrity, CERT-In and DPDP

The rules that shape pharma cybersecurity

Requirement	Frequency / deadline	Source
Good manufacturing practices	MSME deadline 31 Dec 2025 (extension)	Revised Schedule M
Clinical trial conduct and records	In force	NDCT Rules, 2019
Ethics in biomedical research	In force	ICMR National Ethical Guidelines, 2017
Electronic records for US market	In force	US FDA 21 CFR Part 11
Computerised systems for EU market	In force	EU GMP Annex 11
Cyber incident reporting	To CERT-In within 6 hours	CERT-In Directions, 2022
ICT log retention	180 days, in India	CERT-In Directions, 2022
Participant and employee data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025

Key dates on the regulatory timeline

Regulatory Timeline Shaping Pharma Cybersecurity

Key drug, clinical and cross-sector instruments

● In force ● Upcoming (from Oct 2026)

2017	● ICMR National Ethical Guidelines for biomedical and health research
Mar 2019	● New Drugs and Clinical Trials Rules, 2019 notified
Apr 2022	● CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Aug 2023	● Digital Personal Data Protection Act, 2023 enacted
Dec 2023	● Revised Schedule M (Good Manufacturing Practices) notified
Dec 2025	● Revised Schedule M compliance deadline for MSME manufacturers under extension
May 2027	● Most DPDP Rules obligations, incl. breach intimation, take effect

Sources: CDSCO, MoHFW, ICMR, CERT-In, MeitY. Confirm obligations against the official notifications.

Codec Networks

How Codec Networks helps

Research & IP · Clinical privacy · OT security · Data integrity · Vendors · SOC

One partner from lab bench to plant floor



Research & IP Protection

Classification, DLP, insider monitoring



Clinical Data Privacy

EDC, CTMS, CRO assessments



OT Security

Plant inventory, segmentation, MES, SCADA



Data Integrity

Audit trails, access, LIMS, CDS



Cloud & Vendor Assessments

Cloud, CROs, CDMOs, equipment vendors



24/7 SOC

IT and OT monitoring, hunting

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services



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

MSME manufacturers and labs

- IT and plant VAPT (B1)
- Data integrity quick review (B4)
- ISO 27001 gap check (B5)
- Backup and recovery check (B10)

Assurance

Mid-sized manufacturers and CROs

- OT segmentation and assessment (B3)
- LIMS, EDC and QMS testing (B2)
- Clinical data privacy (B6)
- 24x7 managed SOC (B7)

Continuous Resilience

Large pharma and biotech

- IT/OT red teaming (B1, B10)
- IP protection programme (B6, B7)
- SOC with OT signals (B7)
- Board and inspection reporting (B5)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	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

Five new case studies, five broken chains

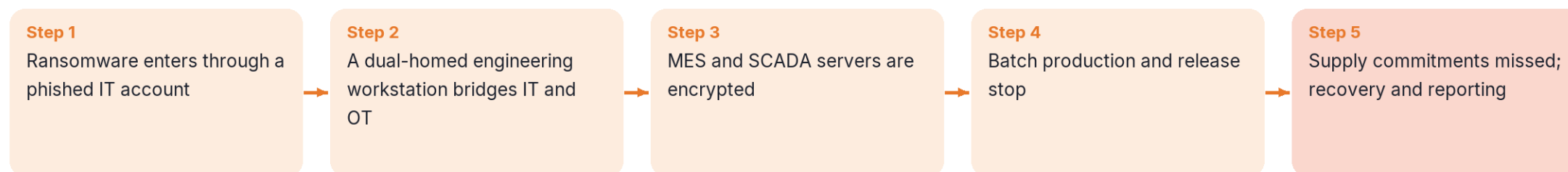
Illustrative composite scenarios written for 2026—not client engagements

1	The Plant That Stopped for a Week	Ransomware crosses into MES and SCADA; segmentation and OT backups limit it	B3 · B7 · B8
2	The Formulation That Left With a Scientist	A departing scientist copies research; DLP and UEBA catch it	B6 · B7 · B8
3	The Trial Data on a CRO's Laptop	A stolen laptop exposes trial data; encryption and oversight prevent it	B9 · B6 · B8
4	The Audit Trail Someone Switched Off	Disabled audit trails fail inspection; data integrity reviews prevent it	B4 · B2 · B5
5	The Research Partner's Shared Drive	Espionage via a partner researcher; MFA and hunting stop it	B9 · B7 · B10

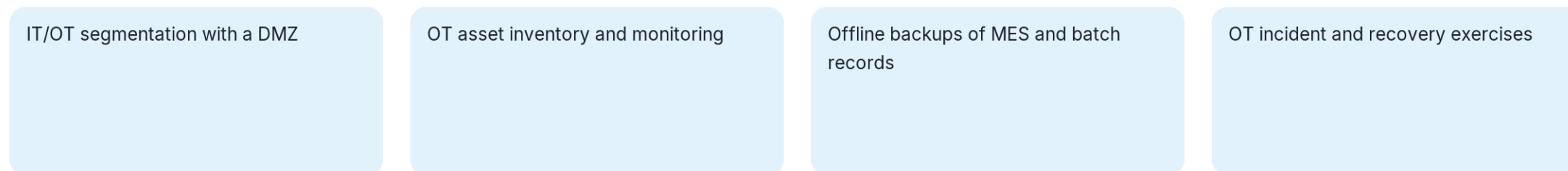
Example: breaking a plant ransomware chain

Case 1: The Plant That Stopped for a Week

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



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

Codec Networks

What we test: phishing resilience, dual-homed systems bridging IT and OT, the IT/OT DMZ, OT asset monitoring, offline backups of MES and batch records, and the recovery and CERT-In reporting steps.

Why pharma companies choose Codec Networks



CERT-In empanelled

For information security auditing services; NISCI empanelled for application audits



Certified

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



Regulation-mapped

Mapped to Schedule M, NDCT Rules, global data integrity, 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 MTDD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Sites, plants, lab and clinical systems, partners and inspection 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.