DivIHN
IN SERVICE, WITH EXCELLENCE AND GRACE

PHARMA & LIFE SCIENCES • SECURITY LEADER FIELD GUIDE

Pharma Pen Testing

GxP, 21 CFR Part 11 & Nation-State Risk

Two regulators are grading your pen testing program.
Only one of them is the FDA.

2
proprietary frameworks: GxP-IP Scoping Matrix + Threat Exposure Index

7
chapters, field-tested against real 2024– 25 pharma incidents

100%
sourced. Every stat and incident appears in the appendix

PHARMA & LIFE SCIENCES • SECURITY LEADER FIELD GUIDE

Table of Contents

AT A GLANCE

What's Inside

This guide builds around two frameworks you can put to work immediately. Real, dated pharma incidents ground every claim, not generic threat commentary.

Framework	What it does
The GxP-IP Dual Scoping Matrix	A 2×2 model that classifies every system by regulatory status and data sensitivity. One pen test engagement can then serve both your FDA compliance risk and your IP protection risk without doubling cost.
The Pharma Threat Exposure Index (PTEI)	A 100-point self-assessment across four axes: third-party access, validated system coverage, dwell-time detection and audit trail integrity. It scores whether a program is defensible, building or early stage.

+50%

rise in FDA CDER warning letters, FY2025 (per FDA's own compliance office)

6–18 mo

dwell time in documented nation-state pharma breaches

27+

pharma and biotech firms exposed by one third-party breach

Read this guide front to back for the full picture. Or jump straight to Chapter 7, score your program first, and work backward into the chapters that explain your weakest axis.

CHAPTER ONE

Two Auditors, One Environment

Your last FDA inspection went well. Your last pen test report came back clean, or clean enough that remediation closed every finding inside its SLA. Your validation team signed off. FDA accepted your 483 response without a follow-up. Your board deck this quarter shows a green box next to “cybersecurity.” None of that confirms whether a state-sponsored actor already holds a foothold in your clinical data repository.

Pharma security leaders operate inside this gap and rarely name it directly. Two auditors evaluate your security program, and they grade different tests. The FDA asks whether your electronic records are attributable, legible, contemporaneous, original and accurate. It asks whether your team validated and tested the systems that create those records in a way that respects their validated state. A nation-state threat actor asks none of that. It asks whether it can reach your synthesis routes, your trial data and your regulatory filing strategy quietly, and hold that access for six to eighteen months before anyone notices.

A pen testing program that satisfies the first auditor often produces exactly the artifact the FDA wants: a scoped, methodical, well-documented test of validated systems that respects their validated state. That same program often produces nothing useful against the second auditor. Standard enterprise pen test scoping centers on asset criticality and network exposure. It never set out to answer whether a compromised CRO credential can move laterally into a research network that a state-sponsored group has mapped for over a year.

ANALYST TAKE

Foundational thoughts

Pharma stands alone in splitting cleanly into two risk frameworks that run in the same environment. A compliance risk framework answers to 21 CFR Part 11 and cGMP. An IP protection risk framework answers to a different fact: intelligence services, not just competitors, target pharma R&D output.
A single, undifferentiated pen test scope satisfies neither framework well. This guide builds a scoping approach around two tracks inside one engagement, and around the specific technical, regulatory and adversarial realities that set pharma testing apart from every other regulated industry.

The chapters ahead follow the order a CISO actually needs: how to scope a test that serves both risk frameworks without doubling cost, how to handle the third-party access paths that carry the most risk, what nation-state actors actually target and how they operate once inside, how to test validated systems without triggering a revalidation event, what FDA's own enforcement data shows about where pharma companies stand today, and a self-assessment framework you can use to score your own program.

> A pen test built to satisfy an auditor and a pen test that would actually stop a state-sponsored actor are not the same engagement.

KEY TAKEAWAYS

✓ Pharma pen testing answers to two independent risk frameworks at once: FDA compliance and nation-state IP protection.
✓ A scope built for one auditor routinely produces nothing useful against the other.
✓ This guide scopes, tests and scores a program against both at the same time.

CHAPTER TWO

Why Standard Pen Test Scoping Doesn't Fit Pharma

One team, two environments, and a scoping model built for only one of them.

Most pharmaceutical companies run one security team across two environments that behave differently. The R&D network exists to move fast. Researchers collaborate with CROs, academic partners and external labs. Data moves through cloud platforms and file-sharing tools. The primary risk here is IP theft by external actors, criminal or state sponsored. The GxP regulated environment exists to stay provably consistent. Systems go through validation, changes go through formal change control, and the integrity of the electronic record carries a regulatory requirement, not just a security preference. A pen test scope that treats these two environments the same way misses what makes each one distinct.

What makes the two environments genuinely different

The distinction goes beyond administration. It changes what "in scope" means, what "active testing" can safely do, and what a finding is worth.

R&D and GxP environments carry different collaboration models, primary risks, compliance regimes and pen test constraints. Each one needs its own scope.

In the R&D environment, IP theft drives the primary risk, and the threat model centers on unauthorized access to high-value research data by external actors. Testing here needs a wide aperture: electronic lab notebooks, LIMS, computational chemistry platforms, genomics repositories and, critically, the collaboration tools that connect internal researchers to external partners. Third-party and CRO access consistently ranks as the highest-priority finding area in R&D scopes. External research partners need broad access, teams document that access poorly after initial provisioning, and few teams review it again. Testing what a compromised CRO credential can actually reach inside the environment often reveals access far broader than security teams expected.

In the GxP environment, data integrity compromise drives the primary risk, and the threat model includes insiders with legitimate system access, not just external attackers. Systems here carry qualification status. An uncontrolled change to a validated system, including a change made purely to remediate a pen test finding, can trigger revalidation. That reality has to shape the engagement from the scoping call onward, not just appear as a caveat in the report. No active testing on production validated systems without an approved qualified test environment. No testing during batch manufacturing runs. Change control documentation for any activity that touches a validated system, even inside a test environment.

The GxP-IP Dual Scoping Matrix

Place every system in the environment into one of four zones, defined by two independent axes: regulatory status (validated or not) and data sensitivity (high-value IP or operational). The methodology, the rules of engagement and the urgency of a finding differ in each zone. A single scope document should specify all four rather than default to one.

	VALIDATED SYSTEM (GxP / 21 CFR Part 11 status)	NON-VALIDATED SYSTEM
HIGH-VALUE IP (formulation, synthesis, trial data)	Zone 1: Regulated Crown Jewels. Qualified test environment required. Active testing mirrors production. Change control before and after. Validation lead signs off on scope.	Zone 2: Exposed Crown Jewels. Standard active testing permitted. This is a priority target because it carries high-value data without validation-driven access friction. Usually the CRO, ELN or LIMS layer.
OPERATIONAL / LOW-SENSITIVITY DATA	Zone 3: Regulated Operations. Qualified test environment required, but findings carry lower urgency than Zone 1. MES, batch records, EBR systems.	Zone 4: Standard Enterprise. Test with standard enterprise methodology. Corporate IT, HR systems, general email.

The GxP-IP Dual Scoping Matrix: four testing zones, one engagement, two risk frameworks.

Zone 1 carries most of the coordination cost: manufacturing execution systems, electronic batch record applications, LIMS instances that create regulated records. Active testing here requires a qualified test environment built to the same specification as production, established before the engagement starts. Zone 2 carries most of the actual IP risk, and teams often scope it lightly because it doesn't carry the same procedural weight as Zone 1: electronic lab notebooks, computational research platforms and the external collaboration layer that connects them to CROs and academic partners. Zones 3 and 4 can run closer to standard methodology, though each should still get its own documentation so remediation ownership stays clear.

Running two scopes as one engagement

Running R&D and GxP as fully separate engagements doubles cost and coordination overhead without improving outcomes. A single engagement with two clearly defined tracks works more efficiently. Each track uses its own methodology, and both tracks test the shared-infrastructure layer, identity management, network backbone and shared file services, in context. The two tracks should report separately. A finding in a validated system triggers a different remediation path, often involving the validation team, than a finding in R&D. Merging them into one findings list creates confusion about ownership and slows remediation on both sides.

FIELD NOTE

What a lightly scoped Zone 2 looks like in practice

When security teams scope pen tests around regulatory status alone, they often miss the access paths that carry the highest IP value: CRO and CDMO connections, research partner file-sharing, and vendor remote access into R&D platforms. These paths sit in Zone 2, carry no validation-driven testing friction, and offer the most direct route to formulation data, synthesis routes and unpublished trial results.

KEY TAKEAWAYS

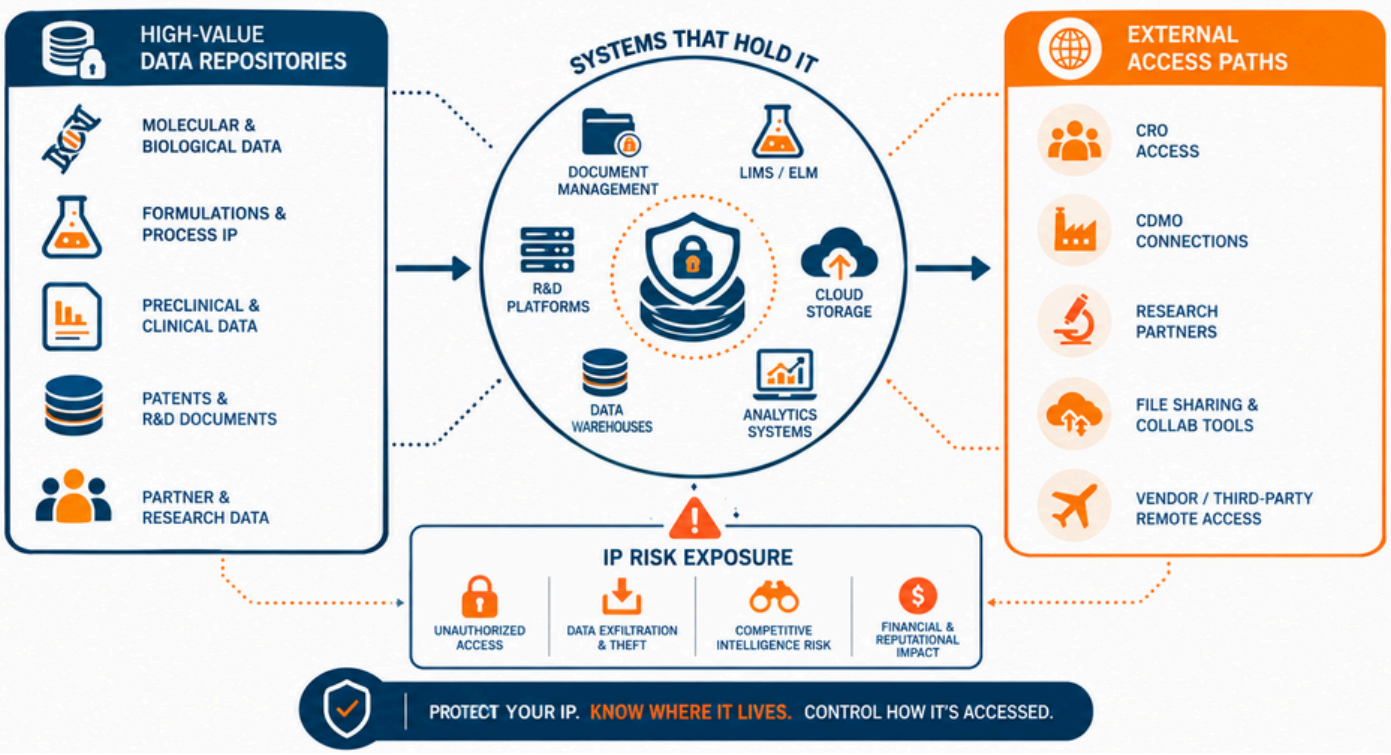
✓ Score every system on two axes: regulatory status and data sensitivity, not one.
✓ Zone 1 (validated plus high-value IP) needs a qualified test environment before anything else happens.
✓ Zone 2 (non-validated plus high-value IP) carries most of the real IP risk, and scopes often underweight it.
✓ Run R&D and GxP as two tracks in one engagement, reported separately, not as two full engagements.

CHAPTER THREE

The Third-Party Blind Spot

The CRO, CDMO or vendor you never pen-tested is the one an attacker already found.

Ask a pharma CISO to name the biggest gap in their pen testing program, and third-party access rarely comes up first. Ask what breached their peer organizations in the last two years, and it comes up almost every time. Contract research organizations, contract development and manufacturing organizations, and laboratory equipment vendors all carry legitimate, standing access into pharma environments that touch high-value IP or patient data. Teams set that access up once, under time pressure, and rarely review it again. It consistently offers attackers the path of least resistance, and pen tests consistently give it less attention than internal systems.



High-value data repositories and the external access paths that reach them: the same systems, viewed from the attacker's side.

Two incidents, one pattern

This pattern is neither hypothetical nor old. Two incidents from the last two years show the same structural weakness playing out at opposite points in the pharma supply chain: a shared services provider and a contract research organization.

FIELD NOTE

Cencora, February 2024 | Pharmaceutical distribution and patient services

Cencora (formerly AmerisourceBergen), a pharmaceutical distributor and business services provider handling a significant share of US drug distribution, disclosed on February 21, 2024 that data had left its systems in an unauthorized transfer. The company's investigation, completed that April, confirmed exposure of patient names, addresses, dates of birth, health diagnoses and prescription data.

The breach did not stay contained to Cencora. At least 27 pharmaceutical and biotechnology companies, including Bristol Myers Squibb, Bayer, Genentech, AbbVie, Novartis, Regeneron and GSK among others, had to notify patients because their outsourced patient support programs ran through Cencora's subsidiary, The Lash Group. One compromise at a shared services provider triggered a disclosure event for over two dozen manufacturers, none of whom directly controlled the systems that got breached.

Source: SEC 8-K filings; BleepingComputer, CPO Magazine, FiercePharma, HIPAA Journal, 2024–2025

FIELD NOTE

Inotiv, August 2025 | Contract research organization

Inotiv, a contract research organization supporting drug development programs for multiple pharmaceutical sponsors, disclosed a ransomware breach by the Qilin group in early August 2025. The breach affected close to 10,000 individuals and involved theft of personal, financial and health information alongside encryption of internal systems.

As a CRO, Inotiv holds exactly the kind of access into sponsor environments that R&D pen test scoping should prioritize. The breach shows what that priority protects against: a compromise at a smaller, less security-mature partner organization can open a foothold into every sponsor that depends on it.

Source: SEC filings; industry breach reporting, August 2025

“One compromise at a shared services provider triggered a disclosure event for over two dozen manufacturers, none of whom directly controlled the systems that got breached.”

Neither incident required a nation-state level of sophistication. Both needed only one thing: a third party with legitimate, standing access to pharma environments that carried weaker defenses than the pharma company itself. That gap shows up often, since smaller distributors, CROs and lab vendors typically run on thinner security budgets. Third-party access testing works best as a named, prioritized track, not a subsection of a broader scope.

What to actually test

→ What a compromised CRO or CDMO credential can reach once inside, not just what it can access on paper.
→ Whether vendor remote access sessions receive the same monitoring rigor as internal privileged access, and whether that monitoring would catch anomalous timing or volume.
→ Whether file-sharing and collaboration tools used with external research partners sit behind proper segmentation from core R&D platforms, or share the same trust boundary.
→ Whether access provisioned for a completed project or expired contract actually gets revoked, not just flagged for review.

KEY TAKEAWAYS

✓ Third-party access draws consistent exploitation and consistently light testing across pharma environments.
✓ Cencora (2024) and Inotiv (2025) both show one weak partner turning into a multi-company disclosure event.
✓ Treat CRO, CDMO and vendor access as a named, prioritized pen test track, not a subsection of the general scope.

CHAPTER FOUR

The Nation-State Playbook

Pharma sits in the same threat category as defense contractors. Most security programs weren't designed for that category.

Pharmaceutical companies sit in the same threat category as defense contractors and critical infrastructure operators. The documentation supporting that claim now extends well beyond a single pandemic-era advisory. Nation-state targeting of pharma predates COVID-19, intensified sharply during it, and has continued since. Standard enterprise security programs rarely catch this level of consistency.

6–18 mo

documented dwell time before exfiltration in pharma breach investigations

~30

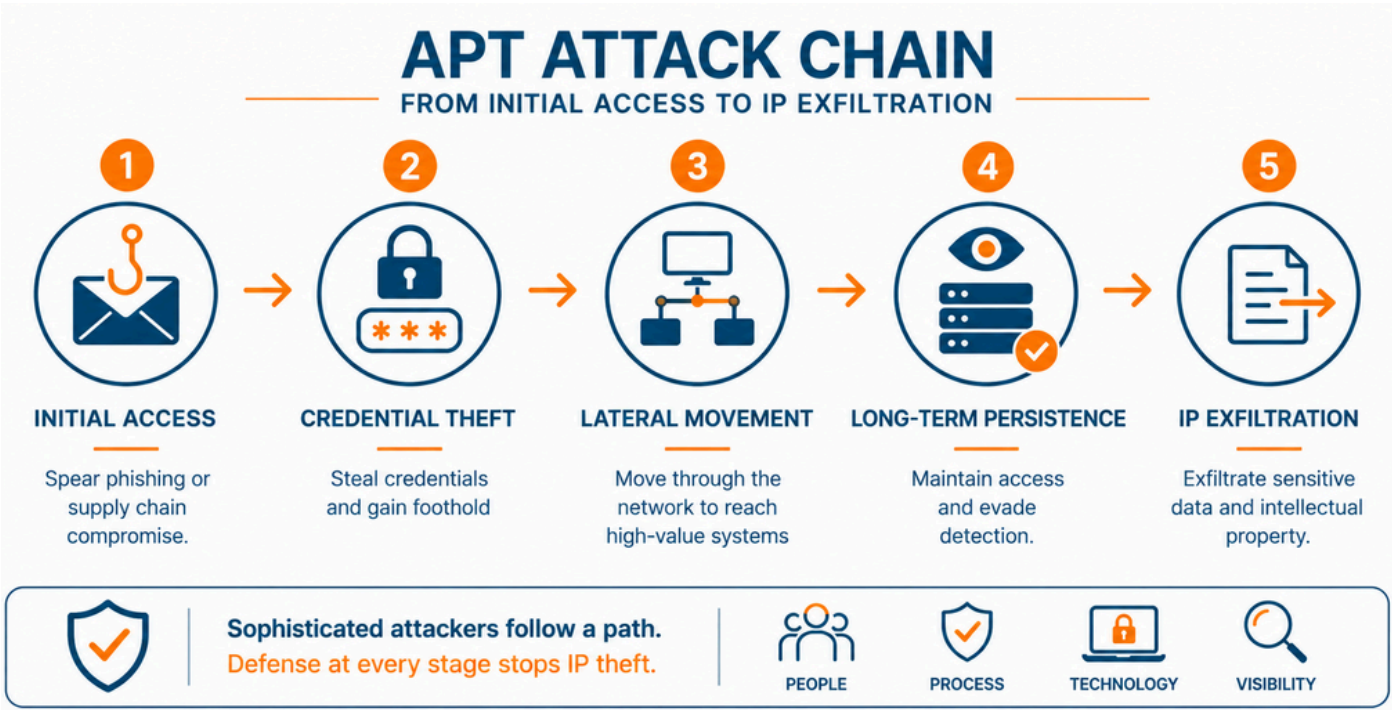
multinational pharma, manufacturing and energy firms hit in one APT41 campaign

Since 2012

APT41 has actively tracked healthcare and pharma targets

What they are after

Nation-state actors primarily target formulation data, synthesis routes, clinical trial results and regulatory filing strategies. Each represents years of R&D investment and carries direct economic value to state-sponsored pharmaceutical industries, plus strategic value to governments managing public health priorities. Secondary targets include manufacturing process IP, which shortens the path to producing branded drugs without the originating R&D spend, and corporate strategy information relevant to acquisition and partnership negotiations.



The APT attack chain against pharma IP: initial access through credential theft, lateral movement, long dwell time, then exfiltration.

Who is doing it, and how

Chinese state-affiliated groups run the most consistently documented campaigns against pharma and biotech targets. APT41 has stayed active against healthcare and pharmaceutical organizations since at least 2012. Researchers have linked the group to an intrusion at a medical device subsidiary and repeated targeting cancer research institutions between 2014 and 2019. A 2022 Cybereason investigation into a campaign researcher named Operation CuckooBees attributed the theft of hundreds of gigabytes of intellectual property, including formulas and proprietary research data, to APT41 across roughly 30 multinational manufacturing, energy and pharmaceutical companies. In September 2022, the HHS Health Sector Cybersecurity Coordination Center issued an alert naming APT41 as an active, ongoing threat to the healthcare and pharmaceutical sector, citing continued use of spear phishing, supply chain compromise, SQL injection and credential theft.

Russian-linked groups intensified pharma targeting specifically during the pandemic period. North Korean groups have distinguished themselves by combining IP theft with ransomware deployment, monetizing the same access in two different ways. Tactically, all three rely on initial access methods that standard controls catch poorly. Spear phishing campaigns against researchers and executives' reference specific research areas, cite real collaborators by name, and mimic legitimate scientific correspondence closely enough to slip past bulk phishing filters. Supply chain compromise forms the second major vector: attackers enter through a CRO, CDMO or lab equipment vendor rather than the pharma company directly, which connects directly to the third-party weakness covered in the previous chapter.

FIELD NOTE

CISA and NCSC joint advisory, May 2020 | COVID-19 pharma and research targeting

US and UK cybersecurity authorities issued a joint alert confirming active investigation into multiple incidents in which threat actors targeted pharmaceutical companies, medical research organizations and universities working on COVID-19 response. The advisory stated plainly that APT groups target such organizations to steal research data and IP for commercial and state benefit.

This was not a one-time pandemic anomaly. It surfaced targeting that predates 2020 and has continued in the years since, documented most recently in the 2022 CuckooBees findings and the September 2022 HHS sector alert.

Source: CISA/NCSC joint advisory, May 2020; Fierce Healthcare

Why they stay hidden, and why detection often misses it

Nation-state actors targeting pharma optimize for persistence, not speed. Investigators have documented dwell times of six to eighteen months before exfiltration across multiple pharma breaches. During that window, attackers map the environment, identify the highest-value data repositories, and build persistence mechanisms designed specifically to survive detection attempts, not just to gain initial access.

Signature-based detection misses this activity almost by design, because attackers use legitimate tools and legitimate stolen credentials. A threat actor using a compromised researcher's VPN credentials to access a clinical data repository at 2am from an unusual location creates a real anomaly, but anomaly detection needs a behavioral baseline first. Many pharma environments have never built one calibrated to actual research workflow patterns. That gap sits in the baseline, not in the tooling.

ANALYST TAKE

What a pen test built for this threat has to test

- Whether credential harvesting from a single compromised endpoint yields access to high-value IP repositories.
- Whether lateral movement from a third-party access point can reach core research systems.
- Whether data exfiltration through legitimate, sanctioned cloud services would register as detectable at all.
- Whether a long-term persistence mechanism, once established, survives the current detection stack without triggering an alert.

This calls for threat intelligence about the specific groups actively targeting pharma, plus adversary simulation that replicates their documented tactics, not a generic vulnerability scan with a pharma logo on the cover page. The output that matters most is an honest answer to how far a real attacker would get, and exactly where defenses would actually stop them.

KEY TAKEAWAYS

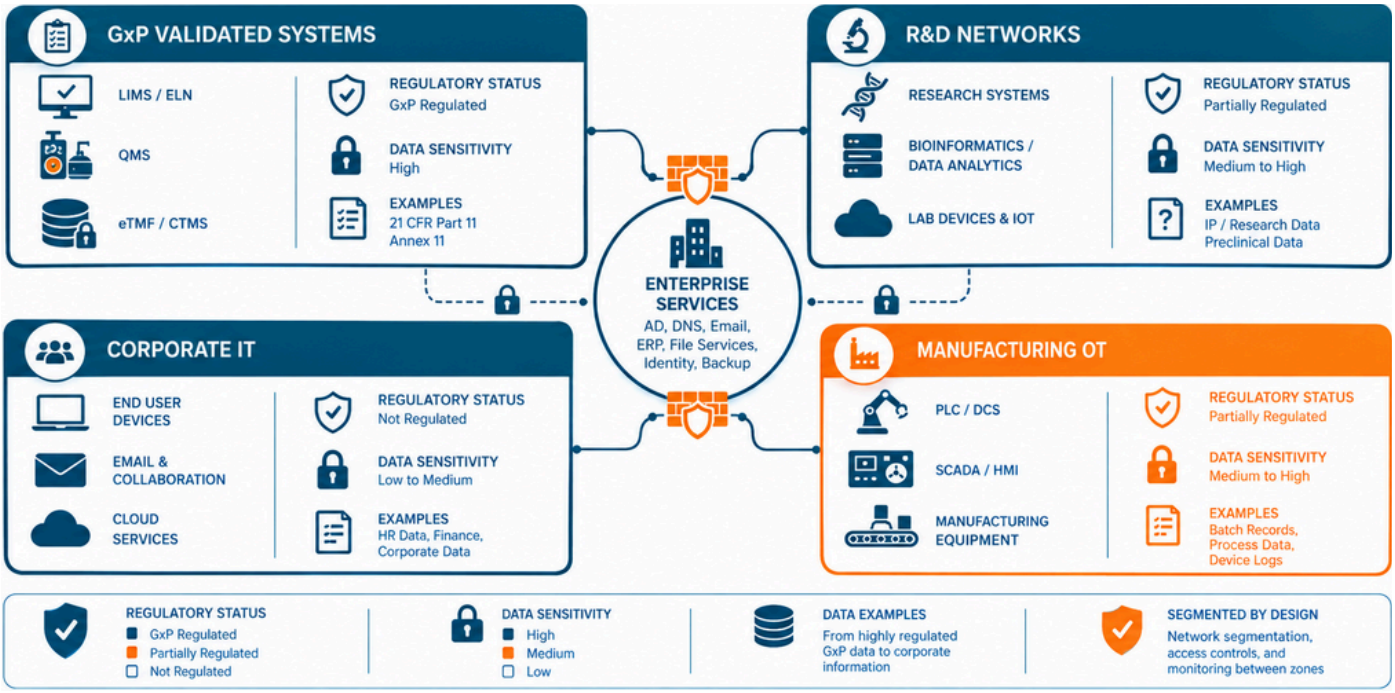
✓ Nation-state actors, APT41 among them, have targeted pharma IP consistently since at least 2012, not just during COVID-19.
✓ They optimize for dwell time, 6 to 18 months, not speed, using legitimate credentials that signature-based tools won't flag.
✓ A pen test built for this threat must test detection, not just exploitation: would the activity even show up?

CHAPTER FIVE

Testing Validated Systems Without Breaking Them

The systems most worth testing are also the ones with the least room for open-ended change.

A single constraint sets pharma pen testing apart from every other regulated industry: the systems most worth testing carry the least room for open-ended change. A manufacturing execution system, a laboratory information management system, an electronic batch record application, or any other system that creates, modifies or stores regulated electronic records under 21 CFR Part 11 and cGMP counts as a validated system. Any change to it, including a change made solely to remediate a pen test finding, can trigger a revalidation event. That reality shapes whether the engagement can run in its default form at all, not just a footnote for the report.



GxP validated systems, R&D networks, corporate IT and manufacturing OT carry different regulatory status and data sensitivity, and sit behind different segmentation boundaries.

The qualified test environment earns its place

For validated systems, a qualified test environment provides the answer: a mirror of the production system, built to the same specification, that can absorb active testing without putting the production environment or its audit trail integrity at risk. Building that environment takes real coordination with the validation team, and it belongs in the project plan before the engagement starts. Finding the need for it mid-scope ranks as the single most common cause of a stalled or trimmed pharma pen test.

Rules of engagement a generic vendor will not anticipate

→ No active testing on production validated systems without an approved, documented qualified test environment.

→ No testing during active batch manufacturing runs, regardless of pressure on the broader project timeline.

→ Change control documentation for any activity that touches a validated system, including activity confined entirely to a test environment.

→ A pre-agreed escalation path for findings that could indicate an active data integrity issue, kept distinct from the standard findings-and-remediation workflow.

These constraints don't reduce what the test can find. They determine whether the findings turn into action or sit as a finding nobody can remediate without opening an unbudgeted revalidation project. A pen test scope document for GxP systems should specify, per system: validation status, the test environment approach, the change control documentation required before and after testing, and the criteria that separate a standard finding from one that needs immediate escalation to the validation team. That level of detail goes beyond a standard pen test scope, and the security team and the validation lead should review and sign off on it jointly before the engagement starts, not after the first finding surfaces.

KEY TAKEAWAYS

✓ A qualified test environment isn't optional for validated systems. It's the only way to test them at all.
✓ Build it into the project plan before scoping starts, not as a mid-project discovery.
✓ Write the escalation path for data-integrity-relevant findings into the scope document up front.

CHAPTER SIX

21 CFR Part 11: The Enforcement Reality

FDA's own enforcement data makes the compliance argument on its own. Warning letter volume is climbing, and manufacturing quality and data integrity failures sit at the center of that increase.

105

FDA warning letters for drug quality issues in FY2024, the highest in five years (+11% YoY)

+50%

year-over-year rise in CDER warning letters, FY2025, per FDA's own compliance office

~35%

of FY2025 CDER warning letters tied to GMP manufacturing failures

FDA's Office of Pharmaceutical Quality reported 105 warning letters for drug quality issues in fiscal year 2024, the highest total in five years and an 11% increase over FY2023. That trend accelerated into FY2025: Jill Furman, Director of CDER's Office of Compliance, told the FDA's 2025 Enforcement, Litigation, and Compliance Conference in December that warning letters issued by CDER rose 50% year-over-year, with roughly 35% tied to GMP manufacturing failures and clinical research and data documentation gaps named among the recurring citation categories.

The specific violations behind these numbers are rarely exotic. They read as mundane and cost real money: manipulated inspection records, missing audit trail entries, inadequate investigation of data anomalies, insufficient process validation. None of these require a sophisticated attacker to create. They point to electronic records and manual data processes that have only faced review on paper, never adversarial testing for whether the controls hold under pressure.

FIELD NOTE

Intas Pharmaceuticals, November 2023 | FDA Warning Letter 320-24-12

FDA's warning letter to Intas Pharmaceuticals, following a May 2023 inspection of its Gujarat, India facility, found that visual inspectors had manipulated particle and defect counts on manual inspection records since 2021 to keep batches within rejection limits, a pattern the agency's letter called “egregious.” The letter also cited inadequate investigation of manufacturing discrepancies and gaps in process validation.

FDA placed the facility on Import Alert 66-40 on November 14, 2023, days before the letter issued, restricting the company's US market access. It was Intas's second warning letter that year: a letter dated July 28, 2023, covering a separate Sanand-area facility cited an analyst who destroyed CGMP records by pouring acetic acid on them, and that site had already been placed on import alert that June.

Source: FDA.gov (Warning Letter 320-24-12); BioSpace, FiercePharma, 2023

ANALYST TAKE

Why this belongs in a pen testing conversation, not just a quality conversation

A validation review confirms that a system meets Part 11 requirements on paper. It doesn't confirm those controls survive an attacker, or an insider, actively trying to defeat them. Audit trail tampering, shared credential exploitation and unauthorized record modification count as security failure modes with regulatory consequences attached. Testing for them belongs in the pen test scope for every validated system, not just in the periodic validation review cycle.

The Intas case shows what this looks like when no one is testing for it: manual records manipulated for two years before an inspector caught it. A pen test built to probe exactly this kind of control gap finds it long before an FDA inspector does, on a timeline the company controls.

KEY TAKEAWAYS

✓ FDA warning letter volume is rising sharply: +11% in FY2024 to a five-year high, then +50% in FY2025.
✓ Roughly a third of FY2025 CDER warning letters trace to GMP manufacturing failures, many involving manual record and data controls.
✓ Validation confirms a system meets Part 11 on paper. It doesn't confirm the controls hold under active adversarial pressure.
✓ Bring audit trail tampering and record modification testing into the pen test scope, not just the validation review cycle.

CHAPTER SEVEN

The Pharma Threat Exposure Index

Turn this guide's central question into a number a board can act on.

Every chapter in this guide circles the same underlying question: does a program stand ready to pass an inspection, stand ready to stop a patient adversary, or both? The Pharma Threat Exposure Index (PTEI) turns that question into a number of security leaders can track, defend to a board, and re-score after each engagement.

Score a program against four axes, each worth up to 25 points, for a maximum of 100.

PTEI Axis	Weight	What "full points" looks like
Third-Party Access Control	0–25 pts	The team maps, scopes and pen-tests CRO, CDMO and vendor access every 12 months as a distinct track, not folded into the general scope.
Validated System Test Coverage	0–25 pts	Qualified test environments cover every Part 11 and GxP system, and the last cycle included active testing, not just a document review.
Dwell-Time Detection Capability	0–25 pts	The environment has a researcher-workflow baseline and can detect anomalous access to IP repositories, not just signature-based malware.
Audit Trail Integrity	0–25 pts	Electronic records meet ALCOA+ standards under active adversarial testing, not just periodic validation review.

Reading the score

Score	Band
85–100	Defensible. The program can substantiate both an FDA inspection and a nation-state-grade red team without structural changes.
60–84	Building. The program passes routine audits. Detecting and containing a patient, persistent adversary needs more work. Most pharma programs land in this band today.
Below 60	Early Stage. The program carries real risk of an undetected dwell-time compromise, a difficult 483 response, or both in the same year.

The PTEI's real value goes beyond the number itself. Scoring honestly surfaces a pattern worth confronting: a program can score well on validated system test coverage, since it passes every FDA-facing metric, and still score near zero on dwell-time detection capability, since no one has built a baseline for normal researcher behavior yet. Those programs carry the most exposure to exactly the kind of six-to-eighteen-month dwell time documented in nation-state pharma breaches. The FDA won't catch that gap. Only a test built to look for it will.

CLOSING

One Scope, Two Adversaries

The FDA and a nation-state threat actor evaluate the same environment from opposite directions. A security program that faces only one of them has already decided which risk it will carry unmanaged. Scoping for a pen test that serves both doesn't double the work of a standard engagement. It builds a single, better scope, drawn from two risk frameworks applied to the same asset inventory, with rules of engagement that respect what sets pharma apart from every other regulated industry it gets compared to.

> **“The organizations getting this right aren't the ones with the biggest security budgets. They're the ones that stopped treating “compliant” and “secure” as the same finding.”**

Start here | Why	Why
Score the program with the PTEI (Ch. 7)	Produces a defensible, board-ready number and points straight at the weakest axis.
Map every CRO, CDMO and vendor access path (Ch. 3)	This is the highest-probability breach path, and the easiest one to scope lightly.
Confirm a qualified test environment exists for every Part 11 system (Ch. 5)	Without it, the highest-risk systems stay untested by default.

APPENDIX

Sourced Incident Timeline

Every incident referenced in this guide, in chronological order, with sourcing.

When	What happened
2014–2020	APT41 (China-nexus) runs sustained campaigns against healthcare, biotech and pharmaceutical targets, including a documented intrusion at a medical device subsidiary and repeated targeting of cancer research institutions.
May 2020	CISA and the UK NCSC issue a joint advisory confirming APT groups are actively targeting pharmaceutical companies, medical research organizations and universities working on COVID-19 response, seeking research data and IP.
May 2022	Cybereason's investigation into “Operation CuckooBees” attributes a multi-year APT41 campaign to the theft of hundreds of gigabytes of IP, including formulas and proprietary research data, from roughly 30 multinational manufacturing, energy and pharmaceutical companies.
Sep 2022	HHS Health Sector Cybersecurity Coordination Center issues an alert reaffirming APT41 as an active, ongoing threat to healthcare and pharmaceutical organizations, citing continued use of spear phishing, supply chain compromise and credential theft.
Jul 2023	FDA issues a warning letter to a separate Intas Pharmaceuticals facility in the Sanand area of Gujarat, India, after an analyst is found to have destroyed CGMP records with acetic acid; the site is placed on import alert that June.
Nov 2023	FDA issues warning letter 320-24-12 to Intas Pharmaceuticals citing an “egregious pattern” of data manipulation dating to 2021 at its Gujarat, India facility, and places the site on Import Alert 66-40.
Feb 2024	Cencora (formerly AmerisourceBergen), a pharmaceutical distributor and services provider, discloses a breach later confirmed to have exposed patient data tied to at least 27 pharmaceutical and biotechnology companies, via a single shared services provider.
FY2024	FDA's Office of Pharmaceutical Quality reports 105 warning letters issued for drug quality issues, the highest total in five years and an 11% increase over FY2023.
Aug 2025	Inotiv, a contract research organization supporting multiple pharmaceutical sponsors, discloses a ransomware breach by the Qilin group affecting 9,542 individuals, underscoring CRO access as a live third-party path into sponsor environments.
FY2025	A senior FDA CDER compliance official confirms warning letters issued by the Center for Drug Evaluation and Research rose 50% year-over-year, with roughly 35% tied to GMP manufacturing failures.

SOURCES & CITATIONS

Direct links to every source cited in this guide. Every link was checked and confirmed live before publication.

1. CISA & NCSC, “APT Groups Target Healthcare and Essential Services,” May 5, 2020 (primary source).
https://www.cisa.gov/uscert/ncas/alerts/aa20-126a

2. CBS News, on Cybereason's “Operation CuckooBees” investigation into APT41, May 2022.
https://www.cbsnews.com/news/chinese-hackers-took-trillions-in-intellectual-property-from-about-30-multinational-companies/

3. SC Media, on the HHS HC3 alert reaffirming APT41 as a healthcare and pharma threat, September 2022.
https://www.scworld.com/analysis/apt41-spear-phishing-supply-chain-campaigns-target-pharma-healthcare

4. FDA.gov, Warning Letter 320-24-12 to Intas Pharmaceuticals Limited, November 21, 2023 (primary source).
https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/intas-pharmaceuticals-limited-662868-11212023

5. BioSpace, on Intas Pharmaceuticals' second 2023 warning letter and import alert.
https://www.biospace.com/intas-pharmaceuticals-hit-with-another-fda-warning-letter-put-on-import-alert

6. HIPAA Journal, on the Cencora data breach and its downstream pharma disclosures, 2024–25.
https://www.hipaajournal.com/cencora-cyberattack-data-breach/

7. FiercePharma, on pharma manufacturers notified through the Cencora breach, May 2024.
https://www.fiercepharma.com/pharma/data-breach-pharma-partner-cencora-leaves-sensitive-patient-information-more-dozen

8. BleepingComputer, on the Inotiv ransomware breach disclosure, December 2025.
https://www.bleepingcomputer.com/news/security/pharma-firm-inotiv-discloses-data-breach-after-ransomware-attack/

9. FDA/CDER Office of Pharmaceutical Quality, 7th Report on the State of Pharmaceutical Quality, FY2024 (primary source).
https://www.fda.gov/media/188236/download

10. The FDA Group, on CDER's FY2025 warning letter increase, citing FDA Office of Compliance Director Jill Furman, December 2025.
https://insider.thefdagroup.com/p/cder-warning-letters-jump-50-percent

ABOUT & GET STARTED

About DivIHN

DivIHN Integration Inc. delivers technology, cybersecurity and workforce solutions to federal, state, local, education and commercial clients. Our penetration testing practice extends across IT, OT and regulated GxP environments, built around the specific compliance and threat realities of highly regulated industries.

DoD TS FCL DOE Q Cleared ISO 9001 ISO 20000 ISO 27001 CMMI DEV | ML 3 APPRAISED SBA 8(a) CERTIFIED

Ready to test what matters safely?

Talk to DivIHN about a pharma penetration testing assessment focused on the risks that matter most, from validated GxP systems and third-party access to high-value IP and nation-state threats.

- www.divihn.com
- Pharma & GxP Security Practice

DivIHN
IN SERVICE, WITH EXCELLENCE AND GRACE

Score the Program, Then Let's Talk

The Pharma Threat Exposure Index in Chapter 7 delivers a defensible starting number. DivIHN's penetration testing team can help close the gap between where that score lands today and where it needs to be.