centrexIT

People-First. AI-Amplified.

LIFE SCIENCES | CYBERSECURITY GUIDE

Securing Operational Technology in Medical Manufacturing

A practical guide to the FDA's 2025 OT cybersecurity white paper, and what it means for your GxP environment.

People-led. AI-amplified. Secure-by-design.

Prepared by the centrexIT Team | 2026

Why this matters now

In June 2025, the U.S. Food and Drug Administration released a white paper on securing the operational technology (OT) used to make medical products. It arrived against a backdrop that every life sciences leader already feels: manufacturing has become the most attacked critical infrastructure sector, ransomware activity climbed sharply through 2025, and pharmaceutical data breaches now carry among the highest average costs of any industry, roughly 4.6 million dollars per incident.

These are not abstractions. In May 2026, West Pharmaceutical Services disclosed a material ransomware attack in an SEC filing, with data exfiltrated and systems encrypted. Weeks later, Novo Nordisk reported a breach that exposed a limited amount of clinical trial information. The pattern is consistent and it is aimed squarely at the sector.

> **Why manufacturing is different**
>
> In most industries a cyberattack is a financial and reputational event. In medical manufacturing it can become a patient-safety event. Production cannot simply restart after an incident. Every system change has to be documented and revalidated first, which is exactly why attackers see regulated environments as high-pressure, high-value targets.

What the FDA white paper is, and what it is not

The document is titled *Securing Technology and Equipment (Operational Technology) Used for Medical Product Manufacturing*. It is important to read it for what it is. It is not a formal guidance document, not a regulation, and it introduces no new mandate. It is a signal.

That signal fills a gap. The FDA has spent years setting expectations for the cybersecurity of devices themselves, both before and after they reach the market. This white paper addresses the missing middle: the environment where those products are made. The agency's message is that you can design a secure device and still put patients at risk if it is produced in a compromised facility.

> **Treat a non-binding paper as a leading indicator**
>
> White papers tend to precede expectations. Procurement is already moving in the same direction, with a meaningful share of healthcare buyers declining purchases over cybersecurity concerns. Acting on this now is cheaper than reacting to it later.

The core problem: OT was built for reliability, not security

Modern production lines run on programmable logic controllers, distributed control systems, and a growing population of connected and smart devices. Most of this equipment was engineered to keep running, not to defend itself. In the FDA's own framing, these technologies have historically prioritized consistent functionality over cybersecurity.

The practical consequence is a visibility gap. It is often difficult to tell what is communicating, when, and where, which makes an intrusion harder to detect and contain. On top of that, commercially available manufacturing equipment frequently does not meet recognized cybersecurity standards by default. Security has to be designed and configured in, deliberately.

The FDA's three categories, translated into action

The white paper organizes its recommendations into three areas. Here is what each one asks of you in practice.

1. Technical Information Exchange, know what you have

- Build and maintain a complete inventory of every connected system on the plant floor, including modules embedded inside other equipment that end users never see.
- Request a software bill of materials (SBOM) from equipment and software vendors so you can trace the security profile of each component.
- Establish visibility into OT network traffic so you can answer what is talking to what.

2. Security Standards and Compliance, align to recognized frameworks

- Map your controls to established standards rather than inventing your own: NIST cybersecurity frameworks, FIPS 140-2/3 for encryption, and CISA best practices.
- Use those frameworks as the shared language between your quality, IT, and OT teams and your auditors.
- Set a baseline configuration standard for new equipment purchases so security is a procurement requirement, not an afterthought.

3. Security by Design, build protection in

- Segment OT networks from IT and from the internet, and use microsegmentation to limit an attacker's lateral movement if they do get in.
- Enforce least-privilege access and strong authentication so the fewest possible people can reach critical systems.
- Monitor continuously for unusual behavior, and design systems so that security and ease of use are balanced rather than traded off.

The hard part: security versus validation

In a GxP environment, the obvious security move, patch quickly, collides with a real obligation: changes to validated systems require change control and revalidation. Attackers know that regulated manufacturers have a low tolerance for downtime, and they use it against you.

You reconcile the two with a risk-based approach:

- Prioritize patching by risk and exposure rather than trying to patch everything at once.
- Where a patch cannot be applied quickly, lean on compensating controls, segmentation and monitoring, to reduce exposure until it can.
- Document every change through your existing change-management process so security work strengthens your quality record instead of threatening it.
- Treat cyber resilience as part of product quality and supply stability, not as a separate IT concern.

Your first 90 days: a starting checklist

You do not have to do everything at once. This sequence turns the white paper into a manageable starting plan.

#	Action	Maps to
1	Build a complete OT asset inventory, including embedded and hidden modules	**Info Exchange**
2	Request SBOMs from your equipment and software vendors	**Info Exchange**
3	Segment OT from IT and from the internet; isolate what does not need exposure	**Security by Design**
4	Enforce least-privilege access and strong authentication on critical systems	**Security by Design**
5	Stand up monitoring for OT network traffic and unusual behavior	**Security by Design**
6	Map your controls to NIST, FIPS 140-2/3, and CISA best practices	**Standards**
7	Adopt a risk-based patching plan that respects change control and revalidation	**Standards**
8	Build and validate an incident response and recovery plan for OT	**All three**
9	Brief leadership: frame cyber risk as a quality, supply, and board-level issue	**All three**

How centrexIT helps life sciences teams

centrexIT has protected regulated and growth-stage organizations since 2002, and life sciences is a core focus of our work. As a Biocom California endorsed partner, we understand the pressure of moving fast on discovery while protecting the systems, data, and manufacturing environments that your reputation depends on.

Our approach is People-led. AI-amplified. Secure-by-design. People who understand your GxP obligations make the decisions; AI gives them the speed and reach to inventory assets, watch OT traffic, and respond to threats faster than an attacker can move. That is how a lean team achieves coverage that used to require a much larger one.

Two ways to start

Take the 2-minute cybersecurity assessment at centrexit.com/cyber-security-readiness-assessment/ for a fast read on where your gaps are. Or book a 30-minute consultation at pages.centrexit.com/free-30-minute-cyber-security-assessment to talk through your OT environment with our team.

Sources

- U.S. Food and Drug Administration, *Securing Technology and Equipment (Operational Technology) Used for Medical Product Manufacturing* (white paper, June 2025).
- FDA Office of Regulatory and Emerging Science, Innovative Technologies page (June 2025).
- BankInfoSecurity / HealthInfoSec, “FDA Urges Medical Product Makers to Beef Up OT Security” (June 25, 2025).
- Industrial Cyber, coverage of the FDA OT white paper and its three categories (June 24, 2025).
- Manufacturing Business Technology, “Cyberattacks Now Threaten Drug Manufacturing Supply Stability” (May 2026).
- IBM, Cost of a Data Breach Report 2025 (pharmaceutical breach cost).
- Honeywell, 2025 Cyber Threat Report (Q1 2025 ransomware increase).
- FiercePharma, “Novo reports data breach, tells clinical trial patients to remain vigilant” (June 2026).