WHITE PAPER
January 2025

# Security Standards in the Pharma & MedTech Supply Chain

PHARMA AERO
WE CONNECT PHARMA

# TABLE OF CONTENTS

# ABSTRACT

Pharma.Aero's Security Standards Project[1] was initiated to address critical gaps in the pharmaceutical and MedTech supply chain's security framework. By tackling the complexity, vulnerability, and fragmentation of current standards, the project identified opportunities for improvement through comprehensive data analysis and stakeholder collaboration.

A comprehensive technical report presenting the detailed findings and actionable guidelines has been shared exclusively with Pharma.Aero members. This white paper offers valuable insights to the entire industry to broaden the project's reach and foster industry-wide engagement. These insights provide a clear path forward for advancing global supply chain security and resilience.

# INTRODUCTION

In recent years, the (bio)pharmaceutical and medical technology (MedTech) sectors have faced growing challenges in maintaining robust security across the entire supply chain. As global demand for pharmaceuticals rises, the supply chain becomes increasingly complex and more susceptible to security risks, threatening the safety, quality, and accessibility of life-saving medications. Additionally, advancements in pharmaceutical innovation, such as personalized medicines (e.g., CAR-T therapies), new technologies (e.g., mRNA vaccines) and radiopharmaceuticals, have introduced new product types that require more specialized and sophisticated approaches to ensure secure handling.

Recognizing these challenges and the need for harmonization, Pharma.Aero initiated the Security Standards project to conduct thorough research of the field and develop a comprehensive security guideline.

With a broad spectrum of stakeholders, ranging from manufacturers to logistics providers and regulatory bodies, the pharmaceutical supply chain operates in a highly fragmented environment. This fragmentation is often compounded by differing security policies, standards, and practices across countries and regions. Without a harmonized approach, inconsistencies can lead to gaps in security, increasing the risk of unauthorized access, tampering, and counterfeiting. The absence of practical and uniform standards not only compromises security but also imposes operational inefficiencies, as companies invest time and resources in meeting disparate regulatory requirements.

[1] https://pharma.aero/pharmaprojects/security-standards/

## Triggers and Drivers for Security Enhancement in Pharma and MedTech

Several factors drive the need for enhanced security within the pharmaceutical and MedTech industries. Regulatory pressures are intensifying as governments and regulatory bodies respond to emerging threats. Stricter requirements for data protection, product safety, and anti-counterfeiting measures demand that organizations continuously improve their security protocols. Additionally, the shift towards digitalization and data-driven decision-making has introduced new cyber risks, particularly regarding data security and asset protection. The pandemic underscored the importance of a resilient and secure supply chain for critical health products, accelerating the adoption of stringent security protocols across logistics operations, from warehousing and transportation to customs and asset protection.

## The Four Security Pillars and Related Security Standards

### AIRPORT SECURITY

Anti-terrorism Security focuses on preventing terrorist activities and ensuring the safety of air cargo through stringent security measures. Compliance with various global and national aviation security programs, along with the IATA Security Management Systems (SeMS), ensures a structured approach to managing security risks in aviation.

### ASSET PROTECTION SECURITY

Asset Protection Security aims to protect pharmaceutical products from theft, damage, and other risks during transportation and storage. Standards such as the TAPA Freight Security Requirements (FSR) and TAPA Transportation Security Requirements (TSR) set guidelines for securing freight and ensuring safe transportation practices.

### CUSTOMS SECURITY

Customs Security ensures that pharmaceutical products comply with customs regulations and are protected from illegal activities during international transport. The Authorized Economic Operator (AEO) Full Certification recognizes businesses that meet high security and compliance standards, facilitating smoother customs procedures.

### DATA PROTECTION SECURITY

Data Protection Security focuses on safeguarding sensitive information related to pharmaceutical products, ensuring data integrity and compliance with privacy regulations. Standards like the General Data Protection Regulation (GDPR) and ISO 27001 provide frameworks for managing information security and protecting data integrity.

# PROJECT STRUCTURE & METHODOLOGY

## Project Structure

| Work Package 1 | Work Package 2 | Work Package 3 | Work Package 4 |
|---|---|---|---|
| Desk Research | Member Interviews | Workshop | Dissemination |

## Project Team

| NAME | ORGANISATION | PROJECT ROLE |
|---|---|---|
| Samuel Speltdoorn | Brussels Airport | BOD Liaison |
| Tanguy Bullier | WFS | Project Lead |
| Joseph Jarman | | |
| Nicola Caristo | n21 Consulting | Project Manager/ Project Expert |
| Anne Julie Verhaeghe | KPMG | Project Manager/ Project Expert |
| Jeremy Xander | | |
| Calle Arvidsson | | |
| Frank Van Gelder | Pharma.Aero | Secretary General |
| Sara Van Lerberghe | | Project Coordinator |
| Alice Iacobescu | | Editorial Review |

## Methodology

The project team adopted a mixed-methods approach, combining quantitative and qualitative methods to gather comprehensive data on the security requirements and challenges in this field. This approach enables a holistic understanding of both the breadth and depth of security complexities, as well as key stakeholder perspectives on achieving a unified security standard.

### Quantitative Design:

A structured, cross-sectional survey was developed to capture industry-wide insights into current security standards, implementation challenges, and compliance with existing frameworks in the pharmaceutical and MedTech supply chains.

### The survey's objectives

- Assess participants' perspectives on the relevance, status, and effectiveness of known security standards,
- Identify common pain points and barriers to compliance
- Collect data on critical security measures prioritized by the industry, particularly for temperature-sensitive, high-value pharmaceuticals

The survey targeted a diverse group of 53 industry professionals spanning executive, logistics, quality assurance, supply chain management, regulatory compliance, and security roles in 39  companies along the supply chain (pharma manufacturers, freight forwarders, airports, airlines, ground handling agents, packaging and cold chain manufacturers, dry ice equipment manufacturers, GSSA for airlines, LS&H packaging, real time visibility and monitoring, other service providers.

## Qualitative Design:

To deepen understanding of the complexities highlighted in the survey, a series of in-depth, semi-structured interviews were conducted with a subset of key stakeholders, targeting senior management and executives. This qualitative component also aimed to capture insights on strategic approaches to enhancing security standards.

### The interviews' focus

- Specific operational challenges associated with current security protocols
- Potential edge cases that require extraordinary security
- Perspectives on critical success factors for a new harmonized tool (e.g. adaptability, interoperability, regulatory compliance)

# RESULTS

## 1. Quantitative Results

The quantitative assessment resulted in a hierarchy of areas where industry professionals see the greatest need for attention to ensure product safety, compliance, and integrity throughout the supply chain.

### Security Areas of Focus

- Access control policies
- Security policy risk assessment
- Air cargo operating procedure
- Data security
- Training policies

The quantitative results reflect some stakeholders' main focus on air and warehousing logistics, which are prioritized in the pharmaceutical and MedTech industries. The variation highlights differing security priorities within the supply chain, with some areas receiving more emphasis due to their impact on safety and compliance.

### Security Certifications and Standards

The industry outreach focused as well on the certification and compliance status across various security, health, and quality standards, segmented by their roles within the supply chain.

1. Pharmaceutical standards (GxP and IATA CEIV)
2. Quality standards: ISO 9001
3. Data security standards: ISO 2700 and GDPR
4. Health and Safety Standards

It is important to note that the survey mentioned only a selection of the many regulations that pharmaceutical and logistics companies must navigate, each varying by region and sector. Additional regulations such as MDR (Medical Device Regulation), DSCSA (Drug Supply Chain Security Act), FMD (Falsified Medicines Directive), serialization and traceability requirements like ICH Q9 (International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use, Guideline Q9 on Quality Risk Management) and GS1 (Global Standards 1), and data protection regulations like HIPAA (Health Insurance Portability and Accountability Act) are also relevant to different stakeholders across the supply chain. This complex regulatory landscape underscores the challenge companies face in ensuring compliance with multiple, often overlapping, standards.

## Varying Drivers for Different Security Areas

In the Pharma and MedTech industries, organizations are motivated to actively engage in various security areas driven by a combination of business, legal, and risk mitigation needs.

**Data security** emerges as a key outlier with the highest combined score, indicating an exceptionally high priority placed on protecting sensitive information, which is critical in the Pharma and MedTech sectors due to the high value and vulnerability of intellectual property and patient data.

Also, the **cargo operation procedures**, which score highly across all categories, reflect the industry's focus on securing products throughout the supply chain, ensuring both regulatory compliance and the integrity of high-value goods.

**Access control policies** also stand out, particularly in risk mitigation, signaling the high importance placed on securing physical access to sensitive areas.
In contrast, auditing practices and training policies appear to be secondary priorities, still viewed as important, while the major focus point is on cargo operations, quality visibility and operational data. Understanding these priorities allows organizations to focus their resources where they can have the most significant impact on securing their supply chain and ensuring compliance.

### End-To-End Commitment To Data Security

The survey and interviews also gathered data regarding the significance of data security within the pharmaceutical and MedTech supply chain, focusing on its prioritization across various security areas. These insights underscore the need for tailored approaches to strengthen data security across diverse operational areas.

| | | | | |
|---|---|---|---|---|
| Air transport security | Access control | Security policy | Training policy | Sea transport security |
| Cargo and personnel screening | Auditing policy | Warehousing | Facility management | Ground transport security |

## 2. Qualitative Results

The interviews revealed a fragmented regulatory landscape, evolving cyber and data security needs, and a growing focus on patient-centricity. Through real-world use cases and expert perspectives, this analysis captures the operational impacts of overlapping standards, the complexities of ensuring data integrity, and the industry's ongoing efforts to balance flexibility with the need for harmonization.

The qualitative findings highlight the fragmented nature of security standards in Pharma and MedTech industries, illustrating both the opportunities for innovation and the pressing need for more integrated, adaptive approaches to meet the demands of a rapidly evolving landscape.

## Diverging Experiences with Security Standards

The survey and interviews also gathered data regarding the significance of data security within the pharmaceutical and MedTech supply chain, focusing on its prioritization across various security areas. These insights underscore the need for tailored approaches to strengthen data security across diverse operational areas.

**Large pharmaceutical companies and established freight forwarders**

- High maturity levels in managing security standards
- Robust, standardized procedures tailored for nearly all supply chain combinations
- Efficient navigation through complex regulatory landscapes
- Consistency and compliance across operations
- High level of security is achieved due to internal company standards, even when certifications are not acquired

**Smaller-sized pharmaceutical companies (e.g., Biotech manufacturers), some contract development and Contract Development and Manufacturing Organizations (CDMO), or companies involved in specialized activities**

- Often lack the resources and expertise to interpret and apply overlapping standards, especially when dealing with region-specific requirements
- Face recurrent challenges such as harmonizing local and international regulations, maintaining compliance, and addressing skill gaps in security management

> “The complexity of regulatory requirements is influenced by a number of factors such as product type (e.g., cell therapy, radiopharmaceuticals, medical device) also impacting storage and transport requirements (e.g., cold chain), transport modes, and the interplay between origin, destination, and supply chain stakeholders. Large organizations with comprehensive lane-specific SOPs are noticeably better equipped to manage certifications and adhere to regulations compared to smaller players.”
>
> **Anne Julie Verhaeghe, KPMG**

## The Growing Priority of Cybersecurity

**Large enterprises**

Cybersecurity is top priority

Investments in cybersecurity protocols, risk assessment frameworks, and data protection strategies

**Small companies**

Broader focus, giving equal weight to both physical security measures and evolving cyber threats

A consistent challenge remains in tailoring cybersecurity strategies to different stakeholders across the value chain, particularly when smaller subcontractors lack the resources or infrastructure to meet stringent standards.

## Underutilization of Available Data

A recurring issue across interviews was the availability of substantial supply chain data that remains underutilized. While companies increasingly recognize the importance of data integrity and traceability, many lack the tools or processes to extract actionable insights from the information they collect. This gap limits the ability to achieve operational excellence, secure interfaces, and reliable end-to-end visibility.

Real-time tracking with clear visibility into every stage of the journey, combined with the ability for stakeholders to take immediate action based on that data, is seen as a key opportunity for improving operational efficiency and security across the industry.

## The Need for Trustable, Secure Systems

The industry also faces a pressing need for systems that facilitate secure, end-to-end information flow while accommodating the diverse requirements of different stakeholders. These systems must ensure stakeholder-dependent access to relevant data, enabling efficient information sharing without compromising sensitive details. For example, the absence of a unified standard for data protection across jurisdictions hinders consistent application and creates vulnerabilities along the supply chain.

Innovations such as digital data exchange platforms aim to address this challenge by enhancing visibility and collaboration while embedding sustainability and security into the process. These platforms represent a step forward in providing tailored, stakeholder-specific access to critical data, fostering trust, and supporting compliance.

> “A data funnel where all data comes in, and one independent organization translates everything from A to B, ensuring that only the involved parties have access on a need-to-know basis, sharing information as needed to provide end-to-end visibility, including both product and commercial data.”
>
> **Eric ten Kate, Ceva Logistics**

## Trust and Harmonization

Despite significant progress in certain areas, stakeholders repeatedly emphasized the need for greater trust and harmonization across the supply chain. Depending on the maturity and size of the stakeholders, there is a lack of universally applicable standards and a common understanding of risk across regions and functions often resulting in inefficiencies and gaps. Addressing these issues requires not only improved frameworks but also a shift toward fostering collaboration among diverse actors in the supply chain ecosystem.

> “Regulatory differences between the EU and the US need to be addressed.”
>
> **Andreas Behnke, Swissport**

# CONCLUSIONS

By combining both quantitative and qualitative data, Pharma.Aero's Security Standards project reveals several key insights into the challenges and opportunities for enhancing security standards in the pharmaceutical and MedTech supply chains. The findings indicate that while stakeholders across the industry are aware of the importance of security, there is a need for efficient alignment, and execution, particularly when it comes to overlapping regulations and inconsistent standards across regions and sub-sectors.

The results suggest a wide variance in the prioritization of security measures among different stakeholders, with larger organizations generally outperforming smaller ones in terms of managing security compliance.

Further, the findings underscore the operational challenges faced by stakeholders in dealing with complex, region-specific security measures. Interviewees highlighted the difficulty in navigating overlapping standards, especially in areas like airport security and customs regulations. The issue of audit complexities was a frequent theme, with many interviewees noting that audits, particularly at airports, can often be redundant and unnecessarily burdensome.

Another crucial finding from both datasets was the heightened emphasis on data protection. Stakeholders expressed the need for secure, end-to-end data management systems that could ensure the integrity of sensitive information, ranging from patient data to shipment tracking details. The use of real-time tracking and secure data exchanges is expanding, yet there remains a critical gap in the availability of comprehensive, interoperable platforms that can securely link all actors in the supply chain. This lack of a unified data ecosystem exacerbates existing security risks.

It is important to note that the survey mentioned only a selection of the many regulations that pharmaceutical and logistics companies must navigate, each varying by region and sector. Additional regulations such as MDR (Medical Device Regulation), DSCSA (Drug Supply Chain Security Act), FMD (Falsified Medicines Directive), serialization and traceability requirements like ICH Q9 (International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use, Guideline Q9 on Quality Risk Management) and GS1 (Global Standards 1), and data protection regulations like HIPAA (Health Insurance Portability and Accountability Act) are also relevant to different stakeholders across the supply chain. This complex regulatory landscape underscores the challenge companies face in ensuring compliance with multiple, often overlapping, standards.

## Next Steps and Outlook[2]

### Adapting to Evolving Regulations

- Stakeholders must stay abreast of evolving regulations like the EU's Falsified Medicines Directive (FMD) and the US Drug Supply Chain Security Act (DSCSA).

- Developing robust change management strategies is essential to ensure compliance and maintain supply chain integrity.

- Efforts should include offering workshops, webinars, and guidance to help organizations implement updates effectively, particularly around serialization and track-and-trace requirements

### Supplier Management and Security Standards

- Building strong, transparent relationships with suppliers to maintain high security standards across the pharmaceutical supply chain.

- Regular audits, performance evaluations, and fostering a culture of accountability to ensure suppliers meet rigorous security standards.

- Special focus on areas such as data security and outsourced functions, including software development.

[1] A more detailed presentation of the project's findings, conclusions, and next steps is available as part of the Technical Report, exclusively for Pharma.Aero members

## Global Logistics Approach

- A coordinated approach across regions to navigate the complexities of the pharmaceutical supply chain while ensuring compliance with local regulations.

- Leveraging pharmaceutical clusters in Europe, North America, and Asia can help enhance efficiency and security through their expertise and infrastructure.

## Strengthening Cybersecurity

- All stakeholders, including logistics providers, must invest in cybersecurity to protect sensitive data and ensure supply chain integrity.

- Business Continuity Plans and regular cybersecurity simulations are critical tools for testing response protocols and preparing for worst-case scenarios.

- Cybersecurity investments also strengthen trust, enhance partnerships, and support the resilience and sustainability of the global supply chain.

## Technological Advancements and Data Integrity

- Real-time tracking and IoT-powered visibility systems ensure shipment data remains authentic and untampered with.

- Adopting interoperable systems to promote transparency, data integrity, and reduce counterfeit risks, while supporting sustainable practices.

By focusing on these key areas, the industry can address emerging challenges and build a more resilient, secure, sustainable, and efficient global pharmaceutical supply chain.
Pharma.Aero will continue to fulfill its mission to foster collaboration and drive positive change in the industry by championing these initiatives and encouraging collective progress.

# ACKNOWLEDGEMENTS

We would like to sincerely thank the project leads for their time and guidance: Tanguy Bullier and Joseph Jarman (Worldwide Flight Services – WFS). Thank you to Samuel Speltdoorn (Brussels Airport), Board Liaison.

Heartfelt thanks go to our Pharma.Aero members taking part in the interviews and sharing valuable insights: Eric Ten Kate (CEVA Logistics), Olivier Mary (Euromed Pharma), Marcus Stoneham (Expeditors), Thomas Zakrzewski (KatalX), Andreas Behnke and Stanislav Bukhman (Swissport), Gergely Szorcsik (Zoetis).

Special thanks to Jeremy Xander, Calle Arvidsson and Anne Julie Verhaeghe (KPMG Advisory BV/SRL), as well as Nicola Caristo (n21 Consulting)  for managing, running the project and bringing expertise, together with the coordination of Frank Van Gelder and Sara Van Lerberghe and the editorial review of Alice Iacobescu.

Pharma.Aero VZW
Bedrijvenzone Machelen Cargo 706B (mailbox 92)
4th floor, room 411
B - 1830 Machelen
Belgium