Strengthening The Healthcare Supply Chain:

Industry Best Practices For Supplier Risk Assessments

HEALTH INDUSTRY DISTRIBUTORS ASSOCIATION

Strengthening The Healthcare Supply Chain: Industry Best Practices For Supplier Risk Assessments

Health Industry Distributors Association (HIDA) member companies work every day to deliver critical products to the nation's healthcare providers at hospitals, nursing homes, physician offices, surgery centers, and the home. Our members work to build a resilient healthcare supply chain to serve patients nationwide.

This paper was produced with federal funds from the U.S. Department of Health and Human Services, Administration for Strategic Preparedness and Response under cooperative agreement number HITEP2100500. The document is not an endorsement of HIDA and does not necessarily represent any agency determination, view, or policy of the U.S. Department of Health and Human Services or its components.

Introduction

Healthcare manufacturers and distributors need adequate visibility across the supply chain to assess risks and build in appropriate safeguards to minimize disruptions. [1] Supply chain disruptions have a negative impact in any industry, and in healthcare, disruptions and shortages affect patient care.

Healthcare products and their components are sourced from around the world, increasing supply chain complexity and risk. To minimize that risk, healthcare distributors and manufacturers typically conduct structured security risk assessments for each of their suppliers before entering into a business relationship, and include contractual protections and remedies to minimize the risk of supply chain disruptions. [2]

To inform efforts to improve healthcare supply chain resilience, the Administration for Strategic Preparedness and Response (ASPR) asked the Health Industry Distributors Association (HIDA) to conduct an analysis of industry best practices of security risk assessments and ways healthcare distributors and manufacturers mitigate risks to the medical supply chain. For the purposes of this paper, the term "supplier" includes suppliers of raw materials to manufacturers as well as manufactured medical products to distributors.

Methodology

HIDA used a mix of qualitative and quantitative research to identify supply chain security assessment best practices. Informed by 10 supply chain security questions identified by ASPR, HIDA conducted a horizon scan of existing literature and government resources. Building from that scan, HIDA created structured qualitative interview guides and quantitative market surveys.

From August 5 through August 29, 2025, HIDA staff conducted qualitative interviews with seven companies and one roundtable discussion that included representatives from five companies. On August 25, HIDA sent the quantitative market survey to key leaders within member companies (390 people total). The survey closed on September 3, with a total of 21 respondents (5% response rate). None of the survey respondents who volunteered contact information (47.6%) had participated in either the qualitative interview or roundtable discussion.

Commercial Supply Chain Security Best Practices

1. Supplier Risk Assessments

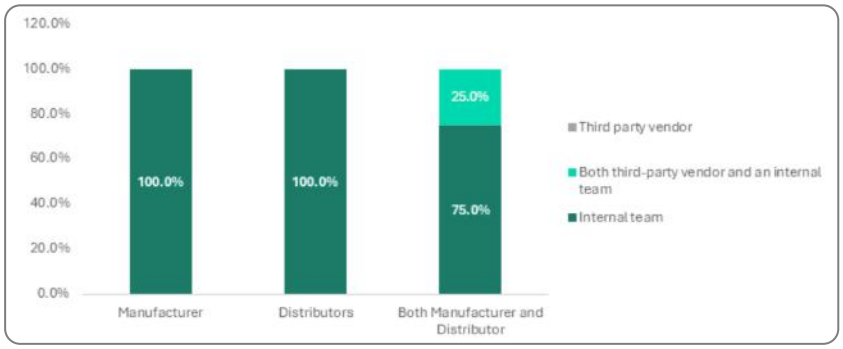

Figure 1 Breakdown of how companies conduct risk assessments.

Conducting supplier risk assessments is a good business practice to protect intellectual property, preserve brand reputation, and mitigate potential legal or financial liabilities. Risk assessments usually occur before a company begins working with a supplier, with periodic re-evaluations after the supplier relationship is established.

Companies use a range of common tools and tactics to assess supplier risk — including proprietary questionnaires, reputational research, site-visits, and third-party scoring — holistically assessing supplier risk. This holistic assessment can be represented in a qualitative risk scorecard to inform leadership of suppliers that may pose a greater risk to the operations of healthcare manufacturers or distributors. For example, some companies will weigh factors gathered from each and assess whether a supplier is "red," "yellow," or "green."

Across HIDA's qualitative interviews, industry leaders emphasized the benefit of forging long-term relationships with suppliers. Several participants noted that these long-term relationships enabled them to have candid conversations about potential delays, disruptions, or other concerns.

A. Proprietary Questionnaires

Risk assessment questionnaires are a common tool for companies to assess supplier risk in a structured way, documenting the supplier's responses to best understand the supplier's ability to meet the requests of the company relying on their products. Manufacturers use these assessments to provide information about raw materials or critical components, and healthcare distributors use these questionnaires to assess the potential risk of suppliers of finished medical products. Additionally, companies will take steps to independently validate responses gathered through the proprietary questionnaire.

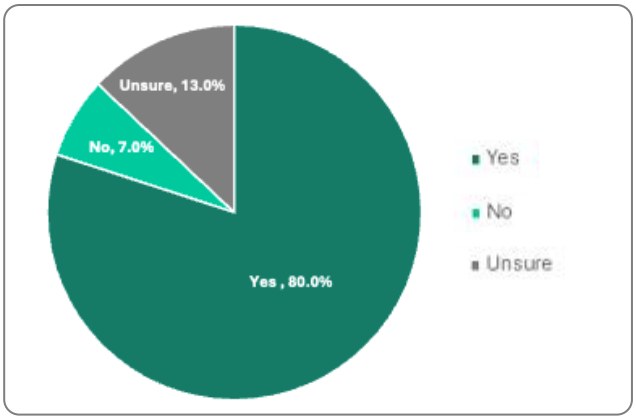

Figure 2 Companies that use a supplier risk assessment questionnaire.

The questionnaires typically include specific questions covering five categories of risk: strategic, operational, financial, geopolitical, and cybersecurity. Based on HIDA's market survey, questions focused on operational, strategic, and financial risk are most common throughout the industry.

- **Operational risks** relate to the supplier's historic performance, including history of on-time delivery of quality products and the supplier's ability to meet fluctuations in demand. HIDA's market survey revealed operational risks as the most common questionnaire category — specifically, the company's history of on-time delivery and adaptability to account for fluctuations in demand.

- **Strategic risks** include risks upstream of the supplier, such as shortages in raw materials or critical components. Establishing whether a supplier has approved alternative sources or an ability to quickly source critical components will mitigate strategic risks. Among surveyed members, assessing a supplier's ability to source alternative raw components quickly, approving alternative sources of critical components, and assessing redundant manufacturing capabilities were common factors to consider in the suitability of a supplier.

- **Financial risks** relate to the overall financial health of the supplier, using factors such as the supplier's solvency and credit score. Customer concentration, where a supplier has a single client representing a significant proportion of their sales, was included as a financial risk by some manufacturers and distributors. Interviewees indicated that customer concentration above 25% of a supplier's sales was a risk, attributing it as a factor of the supplier company's mid-term growth projections.

- **Geopolitical and political risks** include external risks, such as the political stability of where the supplier is located and/or potential risks in transporting the supplier's goods. The COVID-19 pandemic showed the industry that public health emergencies can lead to global shipping disruptions. Throughout 2025, new tariff policies have been a concern for manufacturers and distributors.

- **Cybersecurity risks** include how a supplier proactively monitors its information technology and mitigates cyber threats. Some considerations to reduce cybersecurity risks are whether the supplier regularly trains employees and end users on cybersecurity best practices, establishing appropriate firewalls, and procedures for endpoint detection response.

B. Audits

Distributors and manufacturers conduct audits of their suppliers to validate their understanding of the supplier's capability, capacity, and compliance. Desk audits include validating answers from the risk assessment questionnaire, such as confirming that the supplier has met regulatory requirements.

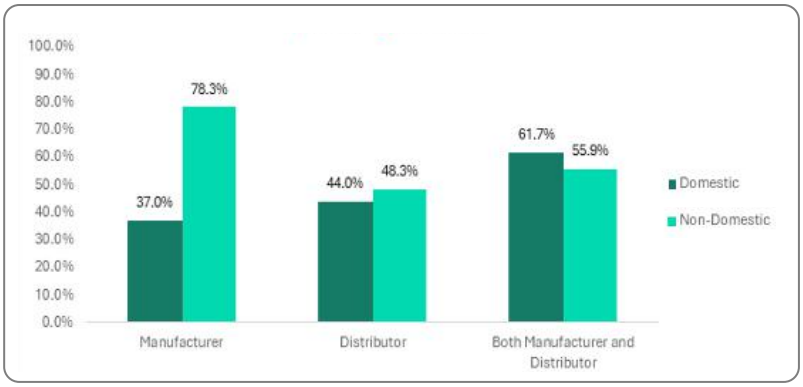

Figure 2 Percentage of supplier audits conducted on-site at a facility.

These audits can include an in-person site visit, particularly if it is a new company or if the supplier has major changes (e.g., company changes ownership). In-person audits are more common for suppliers located outside the United States. Among market survey respondents, 48% conducted in-person audits for domestic suppliers and 58% conducted in-person audits for non-domestic suppliers.

C. Third Party Scoring

Several third-party services will provide risk assessment scores for potential suppliers, particularly in assessing cybersecurity risk. Cybersecurity third-party scoring services, such as those provided by Security Scorecard, offer to make ongoing assessments of an organization's cybersecurity risks and provide a rating. Several interviewees noted that these ratings can be a good datapoint, but caution against over-reliance on these scores because the ratings may be applied without the third-party service validating cybersecurity measures of the supplier.

D. Reputational Research

When assessing a new supplier, companies often conduct independent reputational research.This research can include verifying whether the supplier is subject to ongoing litigation, is connected to disreputable entities or unsavory business practices, or is using a third-party rating of the supplier. Using public databases and internet searches, companies are also able to verify responses from their risk assessment questionnaires. For example, if a healthcare distributor is assessing a new medical device supplier, the distributor would verify that the supplier has 510(k) clearance from the Food and Drug Administration.

This research can include verifying whether the supplier is subject to ongoing litigation, is connected to disreputable entities or unsavory business practices, or is using a third-party rating of the supplier.

2. Contractual Protections

In addition to assessing potential supplier risk, manufacturers and distributors proactively implement contractual protections to mitigate risks in the supply chain. These protections are particularly beneficial in protecting intellectual property, assuring ethical business practices, preventing grey market activity, and protecting proprietary or personally identifiable information.

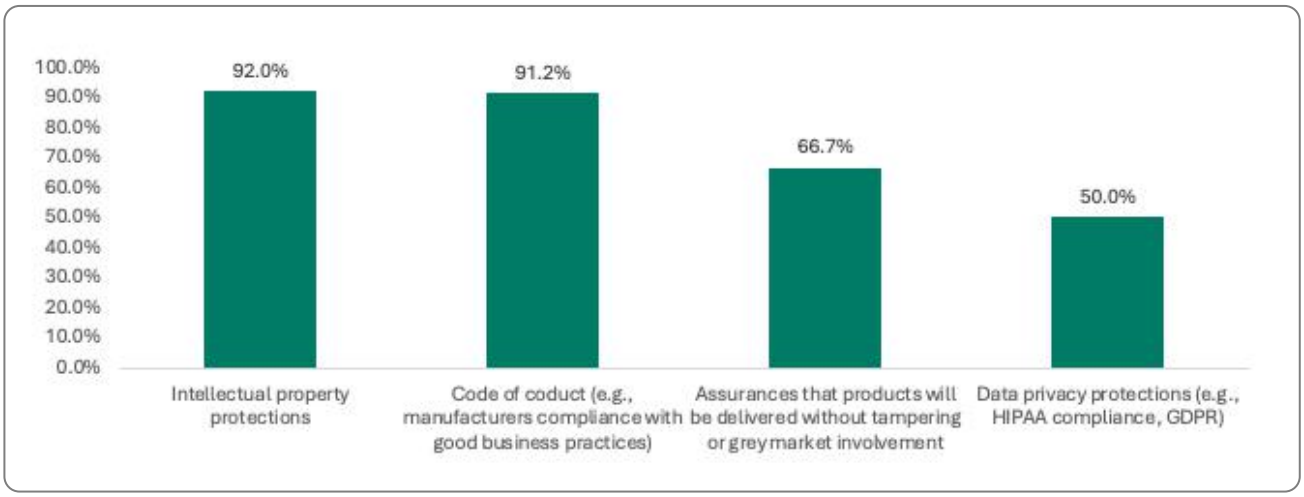

Figure 4 Contractual protections included in distribution agreements.

A. Intellectual Property Protections

Intellectual property protections, such as patents and trademarks, safeguard a company's competitive advantage. Such protections prevent rivals from copying products or ideas, and drive economic growth by building business value, creating jobs, and fostering new markets through licensing and other strategies. Additionally, manufacturers will use contracts with suppliers or with Contract Development and Manufacturing Organizations to protect their intellectual property. [3] Healthcare distributors without a manufacturing business may not have significant intellectual property footprints but will leverage distribution agreements to protect any intellectual property they have.

B. Ethical Business Practice Assurance

Some concerning business practices may not be revealed through the risk assessment process, especially when dealing with a complex network of global suppliers. For example, companies may not have visibility into whether a supplier is connected to an embargoed country [4] or whether the supply chain is connected to illegal practices like the use of forced labor. [5] To protect against these risks, many companies require their suppliers to sign a code of conduct which asserts that the supplier will adhere to certain business practices. [6] These agreements often include assurances that the supplier is not connected to nefarious entities or embargoed nations, assurances that they do not use forced labor or child labor, as well as positive efforts like environmental sustainability and promoting fare wages and working conditions. [7]

C. Preventing Grey Market Activity

Medical supplies are sometimes diverted from authorized healthcare distribution channels for a variety of reasons. This diversion, known as the "grey market," can pose risks to patient care because their path through the medical supply chain is unverifiable. Protections against grey market activity are often included in healthcare distribution agreements. HIDA's market survey showed that 66.7% of companies that manufacture medical products agree to deliver their product without tampering or grey market involvement in their distribution agreements.

D. Data Protections

Sensitive information — financial data, personally identifiable information (PII), and Protected Health Information (PHI) — may flow throughout different aspects of the medical supply chain, necessitating strong data protections. Several legal standards, including the European Union's General Data Protection Regulation (GDPR) which protects PII, and the United States' Health Information Portability and Accountability Act (HIPAA) which protects PHI, govern how companies must handle this sensitive data. HIDA's market survey showed that 50% of companies include data privacy protections, such as assuring HIPAA or GDPR compliance, in their distribution agreements.

Conclusion

Consistently across HIDA's qualitative interviews, companies highlighted the value of forging strong, ongoing relationships with suppliers to both assess and mitigate risk across the medical supply chain. The relationship-centric nature of risk assessments makes them difficult to quantify. Nonetheless, the industry has several best practices in conducting risk assessments:

1. Complete structured security risk assessments supported by a risk assessment questionnaire.
2. Conduct supplier audits, including on-site visits, to best understand supplier capacity and capability.
3. Leverage contractual mechanisms to mitigate risk, including data protections and assurance of ethical business practices.

References

[1] B. Klievink, E. van Stijn, D. Hesketh, H. Aldewereld, F. Heijmann and Y.-H. Tan, "Enhancing Visibility in International Supply Chains: The Data Pipeline Concept," International Journal of Electronic Government Research, vol. 8, no. 4, 2012.

[2] A. Qazi, J. Quigley, A. Dickson and S. Onsel, "Exploring dependency based probabilistic supply chain risk measurers for prioritising interdependent risks and strategies," European Journal of Operational Research, vol. 259, pp. 189-204, 2017.

[3] D. Passmore, "Bridging Innovation and Governance in Biotech," in Becoming a Supply Chain Leader, Productivity Press, 2021, pp. 349-360.

[4] J. Mascaritolo and M. Holcomb, "Moving Toward a Resilient Supply Chain," Journal of Transportation Management, vol. 19, no. 2, pp. 71-83, 2008.

[5] K. Stauss, "Forced Labor in Supply Chains: Addressing Challenges," U.S. Attorney's Bulletin, vol. 65, p. 169, 2017.

[6] Joint Forced Labor Working Group, "Forced Labor Risk in Supply Chains: Considerations for the Healthcare and Public Health Sector".

[7] I. Mamic, Implementing Codes of Conduct: How Businesses Manage Social Performance in Global Supply Chains, London: Routledge, 2017.