NAVEX™

Whitepaper

A Critical Operation: Managing Vendor Relationships in Healthcare

Often indistinguishable from the operations of a given organization—and often afforded a large amount of insider trust and access—third-party entities provide a host of integral services for modern industries. Healthcare is no exception, yet the field's strict regulations, sensitive operating environment, and challenging threat landscape make it especially critical to adopt best practices in managing the risks connected to these vendor relationships.

Fortunately, prudent third-party risk management (TPRM) in healthcare follows a time-tested playbook and hinges on a few key fundamentals that all risk managers can use to assess their organization's progress. It is also a crucial exercise, as studies show that the industry's vendor risk landscape involves serious, ongoing challenges.

TPRM looms large in healthcare

The average modern hospital relies on more than 1,300 external vendors, according to the Ponemon Institute. These third-party entities provide a range of functions, from surgical supplies to billing, and may have varying levels of access to private health information and other sensitive data in order to seamlessly deliver their services.

Some of these vendors offer functionality that is more visible to healthcare users, such as the telehealth services that have seen significant adoption during the COVID-19 pandemic. Others' services are nearly invisible, such as the placement of sensitive patient data in secure off-premise cloud storage.

While IT-related risk is just one area of TPRM, healthcare's regulatory and privacy sensitivities related to data and cybersecurity make it a strong case study in industry risk.

More and more frequently, malicious cyber actors have shown an ability to breach the walls of even very mature, large-enterprise companies. One way of accomplishing this is by overcoming the controls and defenses of third-party service providers that have access to the organization's sensitive systems. Healthcare as an industry endured the greatest share of these third-party attacks in 2021, representing one-third of all incidents, according to Security Magazine.

Healthcare also faced the greatest expenses as a consequence of successful breaches that year, averaging $9.23 million per breach, **according to a report** by Ponemon and IBM. 2021 was the 11th year that healthcare organizations suffered the greatest breach-related expenses across all industries.

The sheer number of third-party vendors for a typical healthcare organization may pale in comparison to an organization like retail giant Walmart, which **said it had more than 100,000 third-party vendors** as recently as 2021. Yet TPRM is a special challenge for risk managers due to the relentless threats healthcare faces and the sensitive nature of its data.

Starting off on the right foot

Despite the complex nature of risks associated with third-party activities in healthcare, the pillars of successful TPRM are relatively simple. The first, effective risk-minded onboarding, is a crucial way to set the tone early with a vendor.

Healthcare organizations should subject all new third-party vendors to a rigorous vetting process involving human resources, procurement, legal, and other teams. This cross-disciplinary group should weigh in on the most important questions to ask regarding several key risk areas, such as:

- ***Finance:*** What are the expenses for using this third party? Is this a prudent use of funds? Are we getting the full value out of this relationship? Do this vendor's services duplicate other services we have in place?
- ***Strategy:*** How important is this vendor for our operations? What would happen if we suddenly lost this third party, and do we have a backup plan in place?
- ***Legal/regulatory:*** What legal or regulatory risks could we face due to this vendor's actions or failures to act? Is this vendor currently subject to sanctions or other regulatory action? What legal agreements are necessary between ourselves and this third party?
- ***Tech/cyber:*** Have we ensured that this third party will only have access to the systems and data necessary for their work? Does this vendor have sufficient information security measures in proportion to the sensitivity of the data they will possess? What would happen if this vendor suffered a breach?
- ***Environment/health/safety:*** Do this vendor's values align with our own? Does our relationship with this vendor create a reputational risk?
- ***Human capital:*** How will this vendor's services impact our existing or future workforce? Will this vendor's services negatively impact morale, recruitment, or retention?

Continuous monitoring is critical

It's not sufficient to consider a third-party risk assessment "done" after a successful onboarding. The landscape of third-party risk is always evolving, sometimes in real time, and healthcare organizations must adopt a few key concepts to identify any newly emerging third-party risk before it is too late.

- ***Recertification of vendors:*** The cross-functional team that weighs in on proper risk assessment methodology should also help determine how frequently a given vendor is subjected to reevaluation. There should be a regular schedule to recertify all vendors, but the interval can depend on the level of risk. Given that every organization has limited resources for risk assessment, a crucial, tier-one vendor whose relationship is critical to operations should be required to recertify their satisfaction of requirements more frequently than a lower-risk, lower-importance third party. The same questions involved in the onboarding process can be a starting point for revalidation, though organizations should also have a regular cadence for updating their focus areas around new operating conditions, regulations, and risks.
- ***Point-in-time inquiry:*** All vendor relationships, but especially critical ones, should include a mechanism whereby risk managers can request short-notice response to inquiry around emerging risks. Keep in mind that third-party suppliers also use third-party services, sometimes known as "fourth parties." Today's fast-moving and complex risk landscape sometimes necessitates an unexpected, emergency huddle with critical vendors to ensure the core organization remains secure.

Complex risk, clear strategy

The dynamics of the healthcare industry present an especially challenging risk landscape involving third-party vendors. While IT risk is only one realm of concern, it is a useful case study for the importance of robust TPRM in healthcare due to the intensity of malicious action and the expensive consequences of a successful breach. Regulatory scrutiny targeting the protection of patient data further emphasizes the importance of TPRM.

Yet for healthcare and all industries, the pillars of a successful TPRM program are relatively straightforward compared to the many dimensions of third-party risk. A cross-disciplinary group is able to ask the right questions during the onboarding process and ensure the cadence of reaffirming that a third-party is complying with certain requirements. Establishing a channel to quickly reach a critical third party and discuss implications of an emerging risk is another important feature of a strong, ongoing TPRM program—one that leads to better protection of patient data.

NAVEX is the worldwide leader in integrated risk and compliance management software and services. Our solutions are trusted by thousands of customers around the globe to help them manage risk, address complex regulatory requirements, build corporate ESG programs and foster ethical workplace cultures.