NAVEX™

Whitepaper

Managing Third-Party Risk is Crucial in Modern Healthcare

By Sal Petriello,
Director of Integrated Risk Management Strategy,
NAVEX

While varying industries rely on third-party vendors for a host of purposes, the financial, regulatory, reputational, and operational pitfalls for healthcare when a third-party incident occurs make third-party risk management (TPRM) an especially important industry focus. As one example of the depth of risk, healthcare as an industry has endured the highest average costs of data breaches across industries for 11 consecutive years, averaging $9.23 million per breach in 2021, according to Ponemon and IBM.

With the average modern hospital relying on more than 1,300 external vendors, according to the Ponemon Institute, today's healthcare organizations face an enduring and increasingly complex challenge in assessing and monitoring third-party risk.

These risks come, however, as key vendors and technologies are offering major opportunities for healthcare delivery and back-office optimization. The recent explosion of telemedicine is just one example of a digital transformation pulling more vendors into the industry. Unseen to much of the public, the trend of moving sensitive patient data to secure, off-premise cloud services is another major transformation in the way healthcare organizations do business. These and other changes to 'business as usual' have served to grow the breadth and depth of third-party involvement in healthcare.

A complex vendor landscape is sweeping the entire industry, from small rural hospitals to massive healthcare organizations. While smaller, rural entities often struggle to attract and retain talent skilled in managing IT- and third-party risk, the fact that those organizations face the same risks of third-party incidents means that no hospital or provider can sidestep the need to effectively manage third-party risk.

Regardless of size or maturity of the healthcare organization, subjecting new vendors to a rigorous vetting process at the onset of the business relationship is crucial. This should be a cross-disciplinary exercise involving Human Resources, Procurement, Legal, and other teams that work together to streamline the vendor validation process. As risk shifts further down the supply chain, this process should also determine how frequently risk managers will require vendors to provide updated information.

Effective and robust initial vetting should determine the level of risk across a number of risk domains, and answer several key questions, such as:

- ***Strategic:*** How critical is this vendor for the operations of my organization and its overall strategic objectives? What would happen if my organization lost this vendor, whether it be by our own decision or something outside of our control?
- ***Financial:*** What is the cost of using this vendor? Does this vendor offer services that overlap with existing capability for my organization?
- ***Legal/regulatory:*** What are the legal and regulatory risks we could face related to this vendor's actions or failures? Is the vendor itself subject to legal or regulatory action? Do we have the proper business agreement in place to address potential risk?
- ***Environmental/health safety:*** Does this vendor's products or services support our own goals for internal environmental, health and safety practices? What would it mean for our organization's reputation if it came to light that this vendor did not match our standards?
- ***Tech/cyber:*** Does this vendor have access to only the information and systems necessary for its work with my organization? Does this vendor have adequate cybersecurity controls in place in respect to the sensitivity of its working relationship with my organization?
- ***Human capital:*** This final risk domain, "human capital," speaks to the impact that a new vendor may have on a healthcare workforce that endured tremendous stress during the pandemic. Each case will be specific to the nature of the vendor relationship. Ask yourself – what impact will this vendor's work have on employee morale, recruitment, and retention?

Effective onboarding is just the first step in minimizing risk from a third-party vendor relationship. Ongoing monitoring is also critical. For business-critical third parties where incidents could result in major damage, more frequent dialogue is important. This includes a depth of business relationship where the healthcare organization can obtain updated information on short notice as new cyberthreats and other risks come to light. Even for lower-risk vendors, a measure of ongoing monitoring remains important. "Lower risk" does not mean "no risk."

While the specifics of third-party risk management can be complex and highly specific to a given organization or vendor, the explosion of third-party vendors in healthcare makes TPRM a non-negotiable obligation for every organization. Understanding some key questions to ask, allies to enlist and risks to assess can be a strong foundation for any healthcare TPRM program. As innovations such as robust telemedicine services evolve, it will only become more important for healthcare organizations to seriously manage the risks involved in these exciting new vendor-driven realms.

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.