Compliance Today - September 2021
You are only as secure as your riskiest vendor

By Kellie Worley, CHC

Kellie Worley (kellie.worley@clearwatercompliance.com) is a Consultant, Professional Services, at Clearwater, located in Nashville, TN.

- linkedin.com/in/kellie-worley-chc-4608835/

As part of a healthcare organization, you are likely well versed in the data privacy and data protection mandates that must be met under the Health Insurance Portability and Accountability Act (HIPAA). If you are a covered entity, you may work with third-party vendors (business associates) that create, receive, maintain, or transmit electronic protected health information (ePHI). Under HIPAA, you need assurances these third-party vendors will safeguard ePHI.

Third-party or vendor risk management is the process of analyzing and controlling risks associated with outsourcing services to third-party vendors or service providers. Many companies have both direct and indirect relationships with third parties that are important to fulfilling business functions or operations, but those outside party relationships also carry significant risks to organizations.

What is the difference between a vendor and a third party? A vendor is an external entity, often in the supply chain, that supplies goods or services to an organization. Examples are:

- Cloud service providers,
- Law firms,
- Accountants/auditors,
- Consultants,
- Software developers, and
- Payment processors.

Third-party relationships encompass all the vendor entities listed above but also include others with whom an organization does business, such as:

- Business partners,
- Venture capitalists, and
- Regulatory agencies.

While many companies have a vendor risk management program, others have more encompassing third-party risk management programs. For purposes of this article, "third party" and "vendor" will be broadly defined to include all entities that have entered a contractual relationship with a healthcare entity to provide business

functions or activities.

Risks imposed by third parties

Third parties are companies that support an organization and often have access to, share, or maintain data critical to business operations. Any company whose employees or systems have access to your systems or data is considered a third party.

When do you have risks from your third-party and vendor relationships? The answer is always. When you work with third-party vendors, their risks are your risks. Here are some of the risks incurred with third-party relationships:

- **Operational risks**: On average, organizations experience about six outages each year related to critical business systems, including patient care systems.
- **Security risks**: Thousands of users can connect to a third-party vendor, and sometimes they can have full access to your network with shared credentials. Security risk is one of the biggest concerns when doing business with third parties. Security breaches of a vendor's systems can result in damage to an organization's own information technology systems and result in disruptions in business processes.
- **Financial and reputational risks**: The global average cost of a data breach is millions of dollars.[1] If a third-party vendor has a violation, an organization can be fined, have operational limitations, and face civil and criminal liabilities.
- **Compliance and regulatory risks**: Under HIPAA, organizations are responsible for securing vendors with access to regulated data. The inability to adequately assess and understand the risks that vendors pose is becoming incredibly costly to healthcare providers.

Challenges in working with third-party vendors

Although the challenges of third-party risk management to a healthcare provider tend to be vast, there are a few prevalent and significant challenges currently within the industry. The number one challenge is adequate resources. Managing third-party risk can be a resource-intensive process, and organizations are not allocating sufficient budget to have an effective vendor risk management program.

The following are a couple of other key challenges that organizations face in the third-party risk management landscape.

Increased security complexities

Third-party cybersecurity incidents are increasing, and a key contributing factor is the growing complexity of the third-party landscape. The number of vendors organizations rely on is increasing at the same time the threats those vendors pose are escalating in frequency and severity. Managing these risks has become an overwhelming problem. For most companies, a reliance on third parties (particularly those that help process data) has become critical for business success.

Outdated models

Another factor challenging third-party risks is that many organizations do not have a coherent process to identify, monitor, and assess the multiple risks posed by third parties. Dealing with third-party vendors for data security and protection is also challenging because it is difficult to enforce compliance externally in the same

way you can within your own organization and with your own employees. There is a false assumption for many organizations that third parties are single-handedly responsible for doing what is required to protect your data. Vendor risk is also often seen as something that exists on its own outside of your organization, so it does not get the same priority as internal risks and issues.

For many organizations, the third-party risk management approach has changed little in recent years, despite the increased complexity of their third-party relationships. Third-party risk management is often fragmented, siloed, or operating with minimal visibility.

Siloed business functions, in which each line of business is responsible for assessing their own vendors, coupled with ineffective tools and incomplete or unsophisticated assessment models, all compound the problem. New approaches to third-party risk management have emerged in recent years, but adoption remains limited to only the highest-performing organizations.

Mature programs have made a concerted effort to centralize vendor risk management so that an approved pool of third parties exists for the entire organization. In midsize organizations, this effectively eliminates the siloes between business functions, reduces duplicative efforts, and sometimes reduces the total number of third parties needed by the organization.