COSMOS
Navigate the Compliance Universe

Complete Healthcare Compliance Manual 2024
Vendor Management Programs: Monitoring Contractor Performance and Proactive Risk Management

By Jiajia Veronica Xu,[1] Esq., CHC, CHPC, CCEP

Why Is It Necessary to Monitor Performance and Manage Risks with Vendors?

Regardless of an organization's line of business, it most likely has vendors that render services or supply goods to support an organization's operations. Vendors, who are generally bound by regulatory requirements and contractual terms and conditions, are essentially the business partners of the organization. To err is human, and vendors are no exception. Although vendors are separate legal entities, their mistakes and errors (including their accidents, incidents, or system breakdowns) can cause significant disruptions and catastrophic damages (i.e., financial, legal, reputational) to an organization's business operations and performance, not to mention the impacts on customers and clients. Debt collection agency Professional Finance Company, Inc., for example, reported in July 2022 that its data breach affected 657 clients (healthcare providers) and involved almost 2 million patients' records.[2][3]

Maintaining proper vendor contracts and knowing the legal obligations are of paramount importance, especially in the event of an incident, so that organizations can ensure regulatory requirements are met, patients protected, and damage mitigated. Business associates are individuals or entities who are not employed by the covered entity but who are given access to protected health information (PHI) to perform certain functions on behalf of the covered entity. If their work includes creating, receiving, maintaining, or transmitting PHI, they are required to sign a business associate agreement (BAA).[4] Although contracts generally are written based on contracting parties' particular needs and circumstances, BAAs have specific legal provisions that must be included. Among these are the scope of the business associate's use and disclosure of the PHI; the appropriate safeguard measures that the business associate implements to protect the PHI; and the business associate's obligation to report any breaches.[5] Given the amount of scrutiny from oversight agencies and the statutory mandates, properly managed vendor contracts are crucial to any organization's compliance with laws and regulations.

Not only will having a comprehensive vendor management program help organizations meet certain legal requirements, it also but will reduce risk exposure, save time by allowing organizations to address issues in a timely fashion, and mitigate any potential damages.

Risk Area Governance

In the healthcare sector, laws and regulations that govern an organization's operations and practices would generally extend to vendors who provide services or goods on behalf of or to the organization, such as exclusion screening, patient privacy and information security, conflicts of interest, and the quality of goods or services. Several laws affect different aspects of vendor management, including exclusion screening, patient privacy and information security, conflicts of interest, and the quality of goods or services.

The Exclusion Statute, 42 U.S.C. § 1320a-7 and 42 U.S.C. § 1320c–5

This federal law prohibits excluded individuals or entities from participating in any federal healthcare program.

Failure to comply with the law may lead to the imposition of civil monetary penalties on healthcare providers that employ or contract with excluded individuals or entities for items or services provided to federal program beneficiaries.[6] Penalties can equal up to $10,000 for each item or service furnished by the excluded individual or entity, as well as an assessment of up to three times the amount claimed.[7]

Health Insurance Portability and Accountability Act, Pub. L. No. 104–191

Although the scope of services and transactions are usually governed by legal contracts between the parties, not all vendors are created equal. Depending on the services and supplies rendered, there are different types of vendors who may not be subject to the same standards, rules and laws. For example, a landscaper or a plumber hired by an organization is not facing the same legal requirements as the organization's radiologist or pharmacist. Various laws and regulations may apply. For example, if a vendor performs work involving the use, transmission, and disclosure of patient PHI on behalf of a healthcare organization, the vendor is likely considered a business associate of the organization. Under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, healthcare organizations (often referred to as covered entities) are required to "enter into written contracts . . . with business associates which *protect the privacy of protected health information*" and the healthcare organization can only disclose PHI to a business associate if the appropriate business associate agreement is duly executed.[8][9] Generally, healthcare organizations are not liable for their vendors' conduct. However, if a covered entity is aware of its business associate's material breach or violation of the contract, "it must take reasonable steps to cure the breach or end the violation, and, if unsuccessful, terminate the contract with the business associate."[10] When termination is not feasible, "the covered entity must report the problem to the Department of Health and Human Services [HHS] Office for Civil Rights."[11] In addition, the Health Information Technology for Economic and Clinical Health Act (HITECH) and the Omnibus Rule also extended HIPAA's privacy and security rules by imposing liabilities and penalties on business associates.

Anti-Kickback Statute, 42 U.S.C. § 1320a–7b(b), and the Physician Self-Referral Law, 42 U.S.C. § 1395nn

In the process of rendering care to patients, healthcare organizations may interact with various types of vendors, which may include other physician practice groups, pharmaceutical companies, and medical device suppliers. Those vendor relations can become problematic if not handled properly; they could involve questionable practices or even illegal activities. Federal laws govern the issue of conflicts of interest. Specifically, the federal Anti-Kickback Statute prohibits the payment or receipt of any remuneration intended to "induce or reward patient referrals or the generation of business involving any item or service payable by the federal healthcare programs."[12] Recently, a distributor of spinal implant devices agreed to pay $1 million to resolve a lawsuit against them. The U.S. Department of Justice Department (DOJ) alleged that the distributor paid physicians to use the medical devices and that the physician-owned distributorships were allegedly vehicles for the payment of kickbacks to induce physicians to use the medical devices in their surgeries. The Anti-Kickback Statute prohibits offering or paying anything of value to encourage the referral of items or services covered by federal healthcare programs.[13] In addition, the Physician Self-Referral Law (Stark Law) prohibits healthcare providers from making referrals to other organizations in which the provider has a financial interest.[14]

False Claims Act, 31 U.S.C. §§ 3729-3733

This federal law may be applied in cases where claims submitted to Medicare or Medicaid for payment are false or fraudulent. The claims can include goods and services. Under this law, no specific intent is required. The standard the law sets is whether the healthcare organization knows or should have known the falsity or fraudulent nature

of the claims. If the organization possessed the actual knowledge of the falsity of the claims or acted in deliberate ignorance or reckless disregard of the truth of the claims, then the organization will be held liable.[15] In other words, if an organization is aware that goods or services rendered by its vendor are substandard and the organization fails to rectify the situation, penalties may be imposed on the organization.