COSMOS
Navigate the Compliance Universe

Compliance Today - December 2022

Jim Passey (jpassey@honorhealth.com) is Vice President, Chief Audit & Compliance Officer at HonorHealth, Scottsdale, AZ.

Tina Daha (tdaha@honorhealth.com) is Compliance Program Manager at HonorHealth, Scottsdale, AZ.

Managing the compliance risk created by third parties

by Jim Passey and Tina Daha

Healthcare organizations rely heavily on third parties to fulfill their missions. Third parties may be represented as suppliers, vendors, contractors, or other individuals or organizations who provide a service or product to a healthcare entity. Working with these parties offers numerous strategic and financial advantages for healthcare entities allowing them to enlist external resources and expertise that would otherwise be significantly more costly for a healthcare entity to provide themselves. The use of third parties is increasing considerably in the healthcare industry, and compliance professionals need to apply appropriate risk management principles to this area. Recent world events have demonstrated the fragility of relying on third parties and the impact they can have on a healthcare entity.

Healthcare entities are required to comply with all federal, state, and local laws, even if a third party conducts the underlying processes. Third parties are typically not owned or operated by the healthcare entity. This separation of ownership and control limits the healthcare entity's ability to ensure compliance with all laws and regulations. If not managed effectively, this could create increased compliance risk to the organization.

The compliance risk of using third parties

Enlisting the assistance of third parties creates a host of potential compliance risks. Generally, third parties are not part of the healthcare entity. They are hired from the outside with minimal awareness of the healthcare entity's policies, culture, norms, and values. Some third-party relations are with individuals in foreign countries who may create language or cultural disparities or operate under different local and national laws. There may also be a question of loyalty to the healthcare entity and its goals. Third-party relations are often focused on short-term opportunities, which means they may not be invested in the long-term good of the healthcare entity. Third parties are generally for-profit entities, which means they may be motivated to increase revenues and cut costs. Such a business philosophy may reduce or eliminate key controls and place compliance as a lower priority.

Compliance risk created by third parties comes in many forms, including compliance with federal and state laws and regulations, privacy laws including business associate arrangements, security laws governing confidential data exchange between parties, Stark and anti-kickback laws related to financial relations with physicians, billing laws governing the processing of claims, licensure and accreditation laws governing appropriate credentialing of clinical and nonclinical licensed professionals, and business relations with foreign countries. *If third parties are not compliant with the host of laws a healthcare organization must comply with, the third-party relationship, directly or indirectly, extends that compliance risk to the healthcare entity.* In many cases, third parties are enlisted as an extension of the healthcare entity itself and are likely required to abide by the same compliance

obligations. Examples of potential risk areas might include temporary workers who are not properly trained on compliance requirements, IT software that creates unintended billing errors, or confusion around which entity is required to notify affected patients if their protected health information is breached.[1] Such risks create direct compliance liability for an organization.

The following are some suggested approaches to managing compliance risk within a healthcare entity. This process may benefit from the assistance of other areas of the healthcare entity as compliance risk may manifest itself in various functional areas such as information security, recruitment, business development, or physician contracting.

Inventory third-party relationships

The first step in managing the compliance risk of third-party relationships is understanding where the organizations' third parties are and how they interact with the organization. Begin by creating an inventory of all third parties. An organization's contracts management database is a convenient place to begin this exercise. Although not all third parties have a contract, most will. This practice will identify various third-party relationships, including vendors, suppliers, contractors, temporary staff, IT service providers, software companies, affiliates, marketing firms, auditors, consultants, law firms, and joint ventures. Consider any individual or entity that is not employed, owned, or operated by the organization with which it conducts business. Beyond the contracts management database, an analysis of payments made through the accounts payable department can help identify third parties who are paid for services but may not be governed under a formal contract.

Additionally, interviews may be held with key stakeholders to identify other possible third parties, including supply chain, procurement, physician relations, operations, and IT. Also of consideration are individuals who may perform some service within the organization voluntarily, such as hospital volunteers, interns, or students, which may also create compliance risk. Housing third-party inventory may be done manually using a simple spreadsheet or logged in a software program designed specifically for this purpose. Once identified, group all third parties into their various categories for ease of ranking the risk they pose to the organization, as described in the following section.

Apply a risk ranking to each third-party relationship

Once third parties are listed, grouped, and sorted, it may be surprising to discover how many third parties the organization conducts its business with. Prioritizing the risk posed by each third-party category will help determine which relations should receive the greatest focus. This risk ranking process may be coupled with the organization's compliance risk assessment process, where emphasis is placed on those areas that pose the greatest compliance risk to the organization and in which areas third parties may be more frequently involved. When risk ranking each category, consider the nature of work being performed. Evaluate the volume of services or products the third party provides in terms of dollars, frequency, or units. Evaluate how the relation potentially impacts compliance requirements unique to the organization. Special risk consideration should be given to third parties that work within the organization's walls, work alongside (or are a replacement for) existing staff or interact directly with patients or customers. Such third parties become the de facto "face" of the healthcare entity; they may pose a greater risk by engaging in activities otherwise conducted by those within its direct control and oversight. The risk ranking methodology should be focused on the compliance dimension of risk and how the relationship impacts the organization. Any risk ranking methodology can be used (e.g., high/medium/low ranking, five-unit scale, etc.). The key is to apply a method that separates those with the highest compliance risk from those with a lower risk thereby informing the risk prioritization process. For example, a third-party relation conducting billing services on behalf of the healthcare entity may rank higher in

the compliance risk ranking than a third-party food vendor. Once the main categories are ranked, individual third-party relationships can be further risk-ranked within the higher risk-ranked categories to prioritize compliance risk management efforts.

Evaluate compliance risk

Once the third parties with the highest compliance risk have been identified, consider conducting an evaluation of the relationship. A compliance risk questionnaire could be created for each category unique to the nature and scope of services or products, focusing on the unique compliance risks posed by that category of third parties. For example, a questionnaire with an IT service provider might include how their employees are trained on privacy and security principles unique to the healthcare industry, what kind of access their employees have to the healthcare entity's systems, and the controls in place to manage secure transmission of confidential data. A questionnaire with a physician group may include questions about how payments are made to ensure compliance with all Stark laws or how fair market value for services is determined. A questionnaire for a joint venture might include determining who is responsible for compliance oversight and whether the joint venture will have its own compliance program or if it will share resources with the healthcare entity.

A general understanding of the third-party's compliance program may also be beneficial. Does the third-party entity have a compliance program in place? Do they conduct routine sanction screens as required in your contracts? Do they educate employees on crucial compliance topics that apply to your entity? How do their employees report compliance concerns? Do they have a reporting hotline? How are matters of compliance risk identified in the healthcare entity reported by third-party representatives? Are there provisions or expectations that the third party cooperate with the healthcare entity's compliance investigations or communicate to the healthcare entity when the third-party conducts compliance investigations internally that could pose risk to the healthcare entity?

As part of this exercise, consider how well compliance expectations are communicated to the third party. Are there provisions in the contract with the third party that hold them accountable for compliance? How are compliance concepts communicated to third parties to ensure they are aware of compliance requirements unique to the healthcare entity's operations? Is the healthcare entity's code of conduct communicated to third-party representatives, and are there expectations for them to follow its precepts?

In its May 2019 publication, "Guidance on the Evaluation of Corporate Compliance Programs," the U.S. Department of Justice emphasized the entity's "rights to analyze the books and accounts of third parties,"[2] which could be added to a risk questionnaire.

Apply compliance risk mitigation actions

Once the compliance assessment results are completed and analyzed, identify areas where risk mitigation efforts would be most effective. If it is determined that essential compliance controls are lacking or nonexistent, create action plans to remedy outstanding concerns. These risk mitigation activities may be incorporated into a broader third-party risk management program already in place in the organization that addresses the full spectrum of risk, including financial, strategic, operational, and reputational. Risk mitigation activities should apply to the nature of the risk exposure identified in the risk evaluation process.

As healthcare entities don't have direct control over their third-party relationships, adopting risk mitigation activities with third parties becomes an exercise in increasing awareness, exerting influence, and motivating and negotiating corrective actions. Third parties may benefit from this exercise in identifying weaknesses in their internal processes which could benefit all parties.

Routine monitoring

Compliance risk is constantly evolving. The landscape of third-party relations within any healthcare entity is fluid, with new third parties being enlisted and past relations changing or expiring. As such, this requires an ongoing compliance risk assessment update to the third-party landscape. Updating third-party inventories, re-ranking risk, and routinely monitoring and applying risk management actions are keys to continually managing compliance risk created by third parties. As quoted in the November 2020 joint publication between the Committee of Sponsoring Organizations (COSO) of the Treadway Commission and Society of Corporate Compliance and Ethics & Health Care Compliance Association, titled *Compliance Risk Management:Applying the COSO ERM Framework*, "the degree of background checking, other due diligence, and compliance-related performance measures should vary based on the assessed level of risk, and due diligence should be repeated periodically as part of maintaining ongoing relationships with high-risk third parties. Due diligence in engaging with certain third parties, as well as ongoing training and monitoring of compliance performance of third parties, have become expected by regulators and are integral elements of this principle."[3]

Conclusion

With the increasing use of third parties to assist in executing its mission, healthcare compliance professionals should create a formal third-party compliance risk management process that appropriately protects the organization from potential compliance risk created by third-party relationships.

Takeaways

- The use of third parties is increasing significantly in the healthcare industry. Compliance professionals should apply appropriate compliance risk management efforts in this area.
- Understand the compliance risk associated with the use of third parties.
- Apply a methodical approach to managing third-party risk in compliance efforts.
- Inventory third parties and prioritize their potential for compliance risk to the organization.
- Assess the compliance controls within high-risk third parties and apply risk mitigation activities, where appropriate.

1 Publication of the OIG Compliance Program Guidance for Third-Party Medical Billing Companies, 63 Fed. Reg. 70138 (December 18, 1998), https://oig.hhs.gov/documents/compliance-guidance/805/thirdparty.pdf.
2 U.S. Department of Justice, Criminal Division, "Evaluation of Corporate Compliance Programs," updated June 2020, https://www.justice.gov/criminal-fraud/page/file/937501/download.
3*Compliance Risk Management: Applying the COSO ERM Framework*, Committee of Sponsoring Organizations of the Treadway Commission, November 2020, 10, https://www.coso.org/Shared%20Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf , https://www.coso.org/Shared%20Documents/COSO-News-Release-Compliance-Risk-Mgmt.pdf.