ahia
Assoc. of Healthcare Internal Auditors

NEW PERSPECTIVES

on Healthcare Risk Management, Control and Governance

www.AHIA.org Journal of the Association of Healthcare Internal Auditors Vol. 40, Number 4, 2021

Show Me the Money!

Audit physician compensation arrangements

page 7

Patient Safety

Ensure a strong culture and commitment

page 13

In Defense of Tattling

Apply the lessons of cheating scandals

page 18

Revenue Integrity Program

Prevent revenue leakage and compliance issues

page 22

Fraud Risks with Vendors

Ensure vendor due diligence

By Victor Hartman, JD, CPA, CFF, CFE

Imagine a scenario where you are responsible for procurement for your hospitals. A pandemic causes a worldwide demand for personal protective equipment (PPE). Is your organization capable of appropriately screening new vendors to ensure quality PPE is procured? Now, this is not such a far-fetched situation to anticipate.

While the effects of Covid-19 on vendor performance are fresh, you must consider other risks. Examples include:

- Your organization decides to outsource part of the information technology department. Is your newly hired vendor taking the necessary precautions to prevent a data breach or stop a ransomware attack?
- Circumstances require an increase in temporary employees in the finance department. How much havoc could an employee with bad intentions create?
- A vendor is retained to enhance your revenue cycle collection efforts. Could this vendor strip Health Insurance Portability and Accountability Act (HIPAA)-protected health information from your files for the purpose of perpetrating a healthcare billing fraud scheme?

The potential frauds that could be committed by temporary employees, vendors or partners are nearly endless. Red flags could alert your organization that foul play is afoot. However, your organization is already responsible for managing a myriad of legal, compliance, data security and patient safety risks. The risks are further complicated because your organization relies on a diverse group of vendors and partners to fulfill its mission. But one additional risk that must not be overlooked is fraud.

Protected health information

One type of vendor due diligence that your organization likely already manages is the risk of losing control of HIPAA-protected healthcare information to a vendor with nefarious intent. A healthcare provider meeting the Department of Health and Human Services' (HHS') definition of a covered entity must comply with the HIPAA rules pertaining to the privacy and security of patient health information. The term covered entity is broadly defined and covers most entities interacting with patients or patient records.

The rules require a business associate of a covered entity to comply with these same rules. In fact, the covered entity must have a written business associate agreement that requires the business associate to comply with the requirements to protect the privacy and security of protected health information. Importantly, a covered entity can be liable for their business associate's HIPAA violations.

A healthcare organization that is taking proactive steps to protect HIPAA health information is already protecting against many identify frauds. Hackers have gotten very adept at attacking healthcare organizations' databases to obtain the personal identity information of patients, employees, customers and other stakeholders. The same due diligence procedures that your organization uses to

vet the vendors who have access to the organization's HIPAA-protected healthcare information can also assist in minimizing fraud incidents with any vendor.

Risk assessment

You need to understand the fraud risks your organization is likely to encounter. Unfortunately, complex healthcare organizations can be exposed to many varied and consequential risks. Begin by identifying the fraud risks through a fraud risk assessment. Then correlate the risks with the parties that could take advantage of the exposures. The parties could include employees and vendors, with the possibility that both parties may be colluding in a fraudulent scheme to defraud your organization.

Conducting a fraud risk assessment can be challenging. Start the risk assessment by brainstorming with key stakeholders and then follow up with questionnaires and interviews of relevant parties to further refine the risk assessment.

Interviews can be a highly effective way to discover fraud risks. Employees and vendors will generally know the fraud vulnerabilities the organization faces. Simply asking these individuals questions as part of a group exercise to conceive of fraud scenarios will often yield surprising results.

The questions can first be geared toward the known fraud risks identified in the brainstorming exercise. Some of the common risks for healthcare organizations are shown in Exhibit 1. How do you discover emerging fraud risks that you are not educated enough to ask about? In this case, try open-ended questions. You might simply ask: If someone were trying to commit fraud, how would they do it?

Exhibit 1 – Healthcare fraud risks

1. Misappropriation of assets
2. Corruption
3. Conflicts of interest
4. Financial statement fraud
5. Theft of intellectual property
6. Information technology vulnerabilities
7. HIPAA information leaks
8. Billing integrity issues
9. Medicare, Medicaid and private pay frauds
10. Stark and anti-kickback issues
11. Code of conduct violations
12. Dealing with Office of Inspector General (OIG)-excluded parties
13. Licensing misrepresentations
14. FDA approval misrepresentations

Vendor identification

After the fraud risks have been identified, correlate them with vendors that are at risk for committing the frauds. Identifying all vendors in a large healthcare organization can be difficult. Start by reviewing the vendors in your accounts payable system. Send a questionnaire to managers who are responsible for the vendors to obtain information to develop a profile on each vendor.

Then develop a process to identify all new vendors. Vendors can then be placed in differing categories for the purpose of identifying fraud risks and the appropriate due diligence procedures that may be needed for that category. Examples of categories are provided in Exhibit 2.

Exhibit 2 – Examples of vendor categories

- Information technology providers
- Temporary service providers
- General services
- Product or equipment providers
- Professional services (e.g., attorneys, accountants, consultants)

Due diligence

Once fraud risks, vendors and vendor categories have been identified, due diligence policies and procedures can be developed to mitigate the fraud risks. In mature organizations, vendor due diligence will likely already exist. You should review those procedures to determine if enhancements are needed to address the fraud risks that have been identified.

Fraud risks should also be evaluated at both the entity level of the vendor and at the vendor employee level for those performing services, installing equipment or delivering products. For example, your organization needs to know the legal entity they will be contracting with and the key executives behind the corporate structure. The information can be obtained by requesting corporate records from the vendor and then validating them with the secretary of state's records or other reference databases. Exhibit 3 summarizes entity-level due diligence.

One of the reasons for understanding a vendor's identity is that your organization should not conduct business with a vendor who has been excluded from participating in a federal healthcare program by the OIG. The effect of an OIG exclusion from federal health care programs is that no federal health care program payment may be made for any items or services furnished by an excluded entity or individual or prescribed by an excluded physician.

Exhibit 3 – Scope of entity-level due diligence

1. Corporate record verification
2. Company background
3. Criminal convictions
4. HHS OIG exclusion and debarment
5. State exclusion and debarment
6. Civil litigation
7. Bankruptcy filings
8. Pending judgments and liens
9. Government sanctions
10. Regulatory violations
11. Social media

The payment ban applies to all methods of federal program reimbursement. Any items and services furnished by an excluded individual or entity are not reimbursable under federal healthcare programs. In addition, any items and services furnished at the medical direction or prescription of an excluded physician are not reimbursable when the individual or entity furnishing the services either knows or should know of the exclusion.

The prohibition applies even when the federal payment itself is made to another provider, practitioner or supplier that is not excluded. If a vendor has already been excluded by the OIG for fraud, that vendor is at a high risk for trying to escape the OIG's reach by subcontracting with a legitimate healthcare organization.

Vendors transact business using employees that deliver the service or product. Accordingly, vendor employees may also need to undergo screening, especially if they conduct work on your organization's premises. Exhibit 4 summarizes employee screening.

Exhibit 4 – Scope of employee screening

1. Past employment verifications
2. Criminal history
3. Credentialing
4. Federal and state exclusion and debarment
5. Driver records
6. Drug testing
7. Social media

Further, products and services need to be assessed to ensure that they meet the contracting terms regarding quantity and quality. The products and services provided should be consistent with the vendor's representations. Exhibit 5 illustrates product or services screening.

Exhibit 5 – Scope of product or service screening

- Food and Drug Administration checks
- Inventory counts
- Equipment testing
- Product or service meets contracting terms

Internet search is your friend. Many of the red flags that might disqualify a vendor can be obtained free of charge through internet searches. Government databases including the HHS OIG exclusion database, your state's secretary of state business database, and federal and state court records can be found online, often at no charge. Many third parties will perform vendor due diligence services as part of a turnkey solution or will work with your organization to develop agreed-upon protocols.

Your organization's due diligence policy should be in writing and shared with vendors. The policy can be placed on your organization's website to ensure its visibility. The management of all vendor policies should include audits to ensure that staff is following the policies. If your organization's staff will not follow policy, why should your vendors?

Your organization's policies and procedures for vendor due diligence may result in a checklist approach for employees to follow. However, a checklist approach should be the result of a thoughtful analytical process.

Summary

Your organization can avoid or mitigate the risks posed by vendors by performing due diligence. Begin the due diligence process by identifying all frauds that could reasonably victimize your organization. Then identify all vendors selling a product or service. The vendors should be grouped into similar categories of risks.

Develop due diligence procedures to address a vendor's organizational-level fraud risks and those associated with the vendor's employees that deliver the products or services. Reevaluate the vendor due diligence process on a periodic basis to address emerging fraud risk schemes. **NP**

Victor Hartman, JD, CPA, CFF, CFE, is Principal of The Hartman Firm, LLC, specializing in forensic accounting and internal investigations. He was an FBI Special Agent. He is now an Adjunct Professor at Georgia State University and serves on Georgia Southern University's Forensic Accounting Advisory Board. Vic can be reached at (404) 369-0616 and Vic@HartmanFirm.com.