MedPro Group
a Berkshire Hathaway company

Checklist

Due Diligence of Business Associates

The healthcare environment is complex, and healthcare organizations of all sizes and types routinely outsource various functions to vendors. Vendors that perform certain tasks or activities that involve the use or disclosure of protected health information (PHI) are considered business associates (BAs).

Because BAs are handling sensitive and confidential data, evaluating them before entering into contracts or arrangements is crucial. Due diligence screening can help ensure that BAs follow ethical standards, federal and state laws, and good practices — and that they will adhere to the healthcare organization's compliance standards. The following checklist can help individuals who are responsible for outsourcing decisions evaluate their due diligence processes for BAs.[1]

	Yes	No
Does your organization conduct risk assessments for potential BAs and categorize them according to levels of risk (e.g., based on the data or systems they will need to access, the importance of the services they will provide, their risk management processes, the types of safeguards they have in place, etc.)?	☐	☐
Has your organization determined what level of due diligence evaluation is required for each category of risk?	☐	☐
Does your organization have written due diligence policies, procedures, and checklists associated with each category of risk?	☐	☐
Have accountabilities for due diligence procedures been assigned, and are staff members aware of their responsibilities?	☐	☐
Are the following evaluation criteria included in the due diligence process: • History, experience, and reputation? • Financial stability? • Physical location (geography) and any associated vulnerabilities?	 ☐ ☐ ☐	 ☐ ☐ ☐

	Yes	No
• Compliance with federal and state laws and ethical standards? • Relevant licenses, registrations, certifications, and inspections? • Hiring and employee screening processes? • Staff credentials and training processes? • Evidence of routine risk analyses? • Business processes and procedures, including use of validated protocols and tools? • Administrative, physical, and technical safeguards (in relation to products, services, and data management)? • Quality control and quality assurance processes and procedures? • Willingness to participate in audits and develop corrective actions? • Documentation processes?	☐	☐
Does your organization evaluate potential BAs for conflicts of interest?	☐	☐
Does your organization require and check all references for potential BAs?	☐	☐
Does your organization conduct site visits for potential and current BAs based on organizational policy and level of risk?	☐	☐
Has your organization identified potential “red flags” as part of the due diligence process (e.g., exclusion from participating with federal healthcare organizations, lack of transparency, inability to produce necessary documentation, vague references, inadequate staffing, and previous criminal or civil penalties)?	☐	☐
Does your organization have processes for addressing red flags during the due diligence process?	☐	☐
When a BA is selected, does your organization enter into a contractual agreement that outlines expectations, services or products provided, compensation structure, privacy/security standards, communication requirements, provisions for oversight and auditing, and documentation requirements?	☐	☐

	Yes	No
Do contractual agreements include or require a separate business associate agreement that meets the minimum necessary requirements set forth by the U.S. Department of Health and Human Services?	☐	☐
Do contractual agreements with BAs require them to certify understanding of, and adherence to, your organization's code of conduct, ethical standards, compliance plan, and any other relevant policies?	☐	☐
Does your organization's legal counsel review all contracts with BAs and work with personnel who are responsible for implementing and managing contracts?	☐	☐
Do personnel who are responsible for managing BA contracts and relationships maintain appropriate oversight (e.g., developing and adhering to audit schedules, keeping current on business and legal changes, and reviewing whether contractual obligations are met)?	☐	☐
Are all due diligence and contract management activities (e.g., initial risk assessments and audits) documented in detail?	☐	☐

Endnote

[1] This checklist is based on information from the following sources: Doyle, M. J. (2011). *Third-party essentials: A reputation/liability checkup when using third parties globally.* Society of Corporate Compliance and Ethics. Retrieved from https://assets.hcca-info.org/Portals/0/PDFs/Resources/library/ThirdPartyEssentials-Doyle.pdf; Iatric Systems. (2014). *Ensuring due diligence with business associates.* Retrieved from https://docs.iatric.com/hs-fs/hub/395219/file-2416185951-pdf/Documents/IatricEnsuringDueDiligenceWhitepaper.pdf; U.S. Department of Health and Human Services, Office of Inspector General & Health Care Compliance Association. (2017, March 27). Measuring compliance program effectiveness: A resource guide. Retrieved from https://oig.hhs.gov/compliance/compliance-resource-portal/files/HCCA-OIG-Resource-Guide.pdf; U.S. Department of Health and Human Services. (2019, May 24). Business associates. Retrieved from www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html; HIPAAtrek. (n.d.). How should I conduct due diligence for vendors and business associates? Retrieved from https://hipaatrek.com/due-diligence-vendors-business-associates/; HIPAA E-Tool. (2020, September 1). *A deep dive — business associate due diligence under HIPAA.* Retrieved from https://thehipaaetool.com/a-deep-dive-business-associate-due-diligence-under-hipaa/