

Due Diligence of Business Associates

In the current complex healthcare environment, healthcare organizations of all sizes and types are increasingly outsourcing 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 healthcare organizations rely on BAs to perform tasks that involve sensitive and confidential data, evaluating these vendors before entering into contracts or arrangements with them 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/evaluations for potential BAs and categorize them according to levels of risk (e.g., based on the types of data and/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.)?	<input type="checkbox"/>	<input type="checkbox"/>
Has your organization determined what level of due diligence evaluation is required for each category of risk?	<input type="checkbox"/>	<input type="checkbox"/>
Does your organization have written due diligence policies, procedures, and checklists associated with each category of risk?	<input type="checkbox"/>	<input type="checkbox"/>
Have accountabilities for due diligence procedures been assigned, and are staff members aware of their responsibilities?	<input type="checkbox"/>	<input type="checkbox"/>

	Yes	No
<p>Has your organization considered the following evaluation criteria (in relation to potential BAs) for inclusion in the due diligence process:</p> <ul style="list-style-type: none"> • History, experience, and reputation? • Financial stability? • Physical location (geography) and any associated vulnerabilities? • 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? • Business processes and procedures, including use of validated protocols and tools? • Technical and physical safeguards (in relation to products, services, and data)? • Quality control and quality assurance processes and procedures? • Willingness to participate in audits and develop corrective actions? • Documentation processes? 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Does your organization evaluate potential BAs for conflicts of interest?	<input type="checkbox"/>	<input type="checkbox"/>
Does your organization require and check all references for potential BAs?	<input type="checkbox"/>	<input type="checkbox"/>
Does your organization conduct site visits for potential BAs and current BAs based on organizational policy and level of risk?	<input type="checkbox"/>	<input type="checkbox"/>
Has your organization identified factors that might be considered red flags during the due diligence process (e.g., exclusion from participating with federal healthcare organizations, lack of transparency, inability to produce necessary documentation, references who provide vague information, inadequate staffing, and previous criminal or civil penalties)?	<input type="checkbox"/>	<input type="checkbox"/>

	Yes	No
Does your organization have processes for addressing red flags during the due diligence process?	<input type="checkbox"/>	<input type="checkbox"/>
When a BA or vendor 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?	<input type="checkbox"/>	<input type="checkbox"/>
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?	<input type="checkbox"/>	<input type="checkbox"/>
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?	<input type="checkbox"/>	<input type="checkbox"/>
Does your organization’s legal counsel review all contracts with BAs and work with personnel who are responsible for implementing and managing the contracts?	<input type="checkbox"/>	<input type="checkbox"/>
Do personnel who are responsible for managing BA contracts and relationships maintain appropriate oversight (e.g., developing and adhering to audit schedules, keeping up to date on business and legal changes, and reviewing whether contractual obligations are met)?	<input type="checkbox"/>	<input type="checkbox"/>
Are all due diligence and contract management activities (e.g., initial risk assessments and audits) documented in detail?	<input type="checkbox"/>	<input type="checkbox"/>

Endnote

¹ 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; HIPAAtek. (n.d.). How should I conduct due diligence for vendors and business associates? Retrieved from <https://hipaatek.com/due-diligence-vendors-business-associates/>

This document does not constitute legal or medical advice and should not be construed as rules or establishing a standard of care. Because the facts applicable to your situation may vary, or the laws applicable in your jurisdiction may differ, please contact your attorney or other professional advisors if you have any questions related to your legal or medical obligations or rights, state or federal laws, contract interpretation, or other legal questions.

MedPro Group is the marketing name used to refer to the insurance operations of The Medical Protective Company, Princeton Insurance Company, PLICO, Inc. and MedPro RRG Risk Retention Group. All insurance products are underwritten and administered by these and other Berkshire Hathaway affiliates, including National Fire & Marine Insurance Company. Product availability is based upon business and/or regulatory approval and may differ among companies.

© 2022 MedPro Group Inc. All rights reserved.