MedPro Group
a Berkshire Hathaway company

Checklist

PATIENT SAFETY & RISK SOLUTIONS

# Due Diligence of Business Associates

In the current complex healthcare environment, it is increasingly common for healthcare organizations of all sizes and types to outsource some functions to vendors. Vendors that perform certain functions 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, it is essential to evaluate these vendors before entering into contracts or arrangements with them. 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 healthcare organizations evaluate their due diligence processes for BAs.

| | Yes | No |
|---|---|---|
| Does your organization conduct risk assessments for potential BAs and categorize them according to levels of risk (e.g., based on the types of data or systems they will have access to [if any], 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 and developed related protocols? | ☐ | ☐ |
| Does your organization have written due diligence policies and checklists associated with each category of risk? | ☐ | ☐ |
| Have accountabilities for due diligence procedures been assigned, and are staff members aware of their responsibilities? | ☐ | ☐ |

| | Yes | No |
|---|---|---|
| Has your organization considered the following evaluation criteria (in relation to potential BAs) for inclusion in the due diligence process: | | |
| • History, experience, and reputation? | ☐ | ☐ |
| • Financial stability? | ☐ | ☐ |
| • 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? | ☐ | ☐ |
| 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 BAs and current BAs based on organizational policy and level of risk? | ☐ | ☐ |
| Does your organization require BAs to produce evidence of a compliance plan and training? | ☐ | ☐ |
| Has your organization identified factors that might be considered red flags during the due diligence process (e.g., lack of transparency, inability to produce necessary documentation, references who provide vague information, inadequate staffing, and previous criminal or civil penalties)? | ☐ | ☐ |
| Does your organization have processes for addressing red flags during the due diligence process? | ☐ | ☐ |

| | Yes | No |
|---|---|---|
| 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? | ☐ | ☐ |
| 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, and compliance plan? | ☐ | ☐ |
| Does the organization's legal counsel review all contracts with BAs and work with personnel who are responsible for implementing and managing the contracts? | ☐ | ☐ |
| 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, reviewing whether contractual obligations are met)? | ☐ | ☐ |
| Are all due diligence and contract management activities documented in detail? | ☐ | ☐ |

## Sources

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

2. 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

3. 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

4. U.S. Department of Health and Human Services. (2013, July 26). Business associates. Retrieved from www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html