**Oversight of Business Associates – Considerations for Compliance**

The *Statewide Health Information Policy Manual* (SHIPM) developed by the Center for Data Insights and Innovation (CDII) provides an analysis of applicable Federal (including HIPAA) and State laws and regulations related to the oversight of business associates (BAs) - *see SHIPM Chapter 4 – 4.4.2 Oversight of Business Associates* for specific information on this topic.

The goal of the oversight program is for the Covered Entity (CE) to ensure a BAs ongoing compliance with the terms and conditions of the business associate agreement (BAA). Departments should consider the following steps/items when establishing their BA oversight program:

* **Create an inventory of all business associates**. Gather a complete list of all business associates – the list should include: the name of the BA, start and end dates associated with the BAA, and contract information for the BA. Departments can use an Excel spreadsheet, database or other tracking method – it is important that the inventory is current and readily available.
* **Assess and document the scope of the business associates’ work and services provided**. For each BA, it is important to understand the scope and nature of the work/services conducted by the BA. Typically there are two types of BAs – (1) “independent contractors” that are conducting their work independently, without extensive oversight by the CE or (2) “agents” acting “as” or “like” workforce members where the CE provides day-to-day oversight and direction. Additionally, documenting the type of PHI/ePHI the BA has access to, creates, and/or maintains provides valuable input for the next step.
* **Evaluate the risk.** Review the information collected about your BAs to determine the overall risk to your organization. For example, a document destruction company that performs the work on sight with oversight is likely less risky than a vendor converting paper health records into an electronic health record system. Take into consideration:
	+ Size and type of the organization - smaller organizations may not have the controls in place for HIPAA, newer organizations may lack the expertise, companies with little health care experience may be unaware of HIPAA regulations, etc.
	+ Scope of work performed – BAs conducting work on your behalf or acting as workforce members are likely more risky.
	+ PHI/ePHI used – BAs with access to more PHI/ePHI are likely more risky than those who have little access.

This information will allow you to categorize your BAs into high, medium and low risk. Maintain any notes, tools, or documents used for evaluation to demonstrate compliance.

* **Establish a program to mitigate all risk levels.** Based on the risk level from the previous step and the sheer number of BAs for your department, determine the oversight program your organization will implement to ensure compliance. Document your risk assessment process and notes you make about each BA – your organization may determine the risk associate with some BAs is acceptable. Consider tailoring your program based on the overall risk level of the BA as well as staff availability, for example:
	+ Conduct onsite visits
	+ Review key documentation (such as policies and procedures, risk assessment)
	+ Conduct interviews with key personnel
	+ Ask BA to complete self-assessment
	+ Require BA to sign letter of “self-certification”
	+ Conduct “pre-negotiation” review/research

Document the goals, strategy, processes and tools associate with your oversight program.

* **Conduct oversight activities.** Once the program is in place, conduct the oversight activities and maintain oversight documentation. Logs, documents, checklists, notes and other documentation should be kept to demonstrate your organization’s compliance.

**Checklist for Compliance**

The following checklist provides a summary of the items needed to demonstrate compliance with SHIPM 4.4.2 Oversight of Business Associates.

| **#** | **Activities / Documents** | **Completed (Y or N)** |
| --- | --- | --- |
|  | Current inventory of all BAs – full list of all BAs including dates associated with BAA |  |
|  | BAA template and log demonstrating continuous review/revisions |  |
|  | BA Risk Assessment – review of all BAs to determine risk level, retain documentation related to the assessment |  |
|  | Documented BA oversight program – including processes, tools, templates, and materials used to perform oversight activities |  |
|  | Documentation of completed oversight activities  |  |