**Statewide Health Information Policy Manual (SHIPM) 4.4.2 – Oversight of Business Associates**

*Compliance Review Tool Question #92*

## Artifact Must Haves and Best Practices

| **Item #** | **Topic** | **Covered (Y or N)** | **Comments** |
| --- | --- | --- | --- |
| 1 | Was documentation (artifact) provided to demonstrate oversight of Business Associates (BA) to verify compliance with requirements of the Business Associate Agreement (BAA) - which may be documented in a Memorandum of Understanding (MOU)? |  |  |
| 2 | Does the artifact(s) identify state entity responsibility for oversight (e.g., PO, SO, HIPAA Privacy and Security team) of the BAA? |  |  |
| 3 | Did the artifact(s) describe a program to periodically review BAAs and verify compliance with all patient privacy and security requirements in the BAA? |  |  |
| 3a | * Is a Risk Assessment completed and documented to determine the overall risk for the state entity? |  |  |
| 3b | * Does the Risk Assessment consider factors to determine the frequency (e.g., size of BA, whether BA accesses health information, length of relationship with BA)? |  |  |
| 3c | * Is there documentation of processes, tools, templates and materials to perform oversight activities? |  |  |
| 3d | * Are the guidelines to document the results of oversight activities? |  |  |
| 4 | Did the artifact(s) demonstrate the state entity has internal controls to: | n/a |  |
| 4a | * Communicate with the BA within 2 days when the state entity receives a request from a patient regarding confidential communications and restrictions on use and disclosure? |  |  |
| 4b | * Identify and evaluate risks with the BA relationship? |  |  |
| 4c | * Identify and include the BAs risks in the state entity’s risk analysis? |  |  |
| 4d | * Demonstrate BA adheres with privacy and security protocols required by law and SHIPM. |  |  |
| 4e | * Verify the BA method to notify the state entity if/when there are any violations of law, policy, or contract occurs (*including breaches or security incidents*)? |  |  |
| 4f | * Document the timeframe the BA has to notify the state entity, when there are any violations of law, policy, or contract occurs (*including breaches or security incidents*)? |  |  |
| 4g | * Document the procedure the state entity takes when it becomes aware of any pattern or practice that constitutes a violation of law and/or BA obligation under the contract? |  |  |
| 5 | Was documentation (artifact) provided to identify all BAs and a list of BAAs, including contracts, MOUs, and IAs that act as a BAA? |  |  |
| 5a | * Does the list include the names of BAs? |  |  |
| 5b | * Does the list include the start and end dates associated with the BAA? |  |  |
| 5b | * Does the list include information related to contract modifications? |  |  |
| 5b | * Does the list include contact information for the BA? |  |  |
| 6 | Does the artifact(s) have official review/acceptance: | n/a |  |
| 6a | * Effective Date? |  |  |
| 6b | * Revision Date? |  |  |
| 6c | * Authorizing Sr./Executive Management Signature? |  |  |

## 

Title(s) of Submitted Policy/Document/Artifact(s) Reviewed:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Stored Location of, or link to Artifact(s) Reviewed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Overall CDII Reviewer Comments:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of CDII Reviewer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date Reviewed: \_\_\_\_\_\_\_\_\_\_\_\_

Title of or link to Other Source(s) used (e.g., sources not in checklist, templates) – *optional*:

[OCR Guidance on BAA](https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html) – including template – can be found at the following web address:

www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html