**Statewide Health Information Policy Manual (SHIPM) 4.4.1 – Business Associate Agreement**

*Compliance Review Tool Question #91*

**Artifact Must Haves and Best Practices**

| **Item #** | **Topic** | **Covered (Y or N)** | **Comments** |
| --- | --- | --- | --- |
| 1 | Does the language of the BAA artifact(s) between a covered entity (organization being reviewed) and a business associate include the following:  | n/a |  |
| 1a | * Establish the permitted and required uses and disclosures of Health Information by the Business Associate?
 |  |  |
| 1b | * Identify the purpose for the permitted disclosures?
 |  |  |
| 1c | * Provide that the Business Associate will not use or further disclose the information other than as permitted or required by the contract or as required / permitted by law?
 |  |  |
| 1d | * Require the Business Associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic Health Information?
 |  |  |
| 1e | * Requirement that the Business Associate provide privacy and security awareness training to their workforce (including vendors and subcontractors)?
 |  |  |
| 1f | * Requirement that workforce complies with all applicable state and federal requirements and the BAA, MOU or IA?
 |  |  |
| 1g | * Requirement the Business Associate report to the Covered Entity any use or disclosure of the information not provided for by its contract, including security incidents and breaches of Health Information?
 |  |  |
| 1h | * Identify the specified timeframe to report to the Covered Entity any use or disclosure of information not provided for by it contract to ensure the state entity complies with their reporting and notification requirements?
 |  |  |
| 1i | * To the extent the Business Associate is to carry out a Covered Entity’s obligation under the Privacy Rule, require the Business Associate to comply with the requirements applicable to the obligation?
 |  |  |
| 1j | * Require the Business Associate to make available to CalHHS its internal practices, books, and records relating to the use and disclosure of Health Information received from, or created or received by the Business Associate on behalf of, the Covered Entity for purposes of CalHHS determining the covered entity’s compliance with the HIPAA Privacy Rule?
 |  |  |
| 1k | * Include a provision immediately terminate the Agreement if Business Associate has breached a material term of this agreement and cure is not possible?
 |  |  |
| 1l | * At termination of the contract require the Business Associate to return or destroy all Health Information received from, or created or received by the Business Associate on behalf of, the Covered Entity (*if feasible*)?

(*if return/destruction of Health Information is not feasible, does the artifact(s) require the BA to extend the protections of the BAA, MOU or IA to the Health Information and limit further uses and disclosures*) |  |  |
| 1m | * Requirement that the Business Associate ensure any subcontractors, it may engage on its behalf, that will have access to Health Information agree to the same restrictions and conditions that apply to the Business Associate with respect to such information?
 |  |  |
| 1n | * Authorize termination of the contract by the Covered Entity, if the Business Associate violates a material term of the contract?
 |  |  |
| 2 | Does the artifact(s) require the Business Associate to disclose Health Information as specified in its BAA to satisfy:  | n/a |  |
| 2a | * A covered entity’s obligation with respect to individuals' requests for copies of their Health Information?
 |  |  |
| 2b | * Make available Health Information for amendments (and incorporate any amendments, if required)?
 |  |  |
| 3 | Does the Business Associate Agreement (BAA) artifact(s) include a requirement that all Business Associates document, track and account for all disclosures required to comply with an Accounting of Disclosures?  |  |  |
| 4 | Does the BAA artifact(s) address how and when (timeframe) the Business Associate is to provide the state entity with the information necessary to comply with the 60 day response time requirement for an accounting when requested by the patient? |  |  |
| 5 | Does the BAA provide for communication from state entity to BA (and vice versa) regarding confidential communication to patient, and restrictions on disclosures? |  |  |
| 6 | Did the artifact(s) demonstrate the state entity has internal controls to: | n/a |  |
| 6a | Update existing BAAs when there is a change in law that affects the requirements in the BAA? |  |  |
| 6b | Periodically review the BAA template and update to ensure the template is accurate and consistent with the law? |  |  |
| 6c | Periodically distribute the BAA template to all units in the state entity to ensure the correct template is being used? |  |  |
| 7 | Does the artifact(s) have official review/acceptance: | n/a |  |
| 7a | Effective Date? |  |  |
| 7b | Revision Date? |  |  |
| 7c | Document the authorizing (senior or executive) management approval? |  |  |

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