**POLICY & PROCEDURES**

***Defining the Overall Approach toward Meeting a Requirement***

### **Business Associate Contracts and Other Arrangements §164.308(b)(1),**

**§164.308(b)(2), §164.308(b)(4), §164.314(a)(2)(i), §164.314(a)(2)(iii)**

### **Effective Date:** <Month Day, Year>

### **Policy Number:** <If applicable> **Rev.** 0

**Policy:** When another entity is acting as a business associate for our organization, the business associate must appropriately and reasonable protect the ePHI that is creates, receives, maintains or transmits on our behalf. We also allow our business associates to permit a business associate that is a subcontractor to create, receive, maintain, or transmit ePHI on our behalf. We require both entities to appropriately safeguard the confidentiality, integrity, and availability of ePHI in compliance with the HIPAA Security Rule.

**Procedures:** We will permit a business associate to create, receive, maintain or transmit ePHI on our behalf only if there is a written agreement between the two parties that ensures that the business associate will appropriately and reasonable safeguard the information. We must make a good faith attempt to obtain satisfactory assurances that the business associate will safeguard our ePHI as required by the business associate contract, and to document the attempt and the reasons if these assurances cannot be obtained. Similarly, we will allow our business associates to permit a business associate that is a subcontractor to create, receive, maintain, or transmit ePHI on our behalf only if the same requirements as above are met.

Our Security Official will obtain a signed business associate contract with companies or persons we hire to handle ePHI on our behalf. This contract will have the proper and appropriate language mandated by the HIPAA Security Rule regardless of which entity created the contract document. These contracts will be reviewed annually and securely maintained.

**Details:** The business associate contracts and other arrangements procedures include but are not limited to:

* Identify all business associates who create, receive, maintain, or transmit ePHI on our behalf.
* Sign a written business associate contract that complies with the HIPAA Security Rule with each business associate. When a business associate refuses to sign our business associate contract we will sign the vendor’s contract if the contract contains the proper and appropriate language mandated by the HIPAA Security Rule.
* Review existing business associate contracts to ensure they still comply with the HIPAA Security Rule (last revised on January 25, 2013) and update any contracts that are not compliant on an annual basis.
* Advise applicable business associates who provide our ePHI data to a subcontractor that they are required to have HIPAA-compliant Business Associate contract signed with their subcontractors to address the confidentiality, integrity, and availability of ePHI if no contract has been signed.
* Obtain written due diligence assurances from all business associates regarding their compliance with the HIPAA Security Rule. The following types of questions will be used to acquire this information:
* During the last 12 months, has the business associate conducted a HIPAA security risk assessment for the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information?
* Has the business associate signed your business associate contract or have we signed their contract that complies with the 2013 HIPAA Final Rule?
* Does the business associate have written policies and procedures that address and comply with the HIPAA Breach Notification Rule and the Security Rule’s administrative, technical, organizational and physical safeguard requirements?
* Has the business associate implemented a HIPAA-compliant security awareness and training program and trained all employees and contractors?
* Does the business associate’s IT services meet HIPAA compliant security standards for protecting electronic protected health information?
* Obtain written due diligence assurances from each business associate who uses a subcontractor(s) regarding their subcontractor’s compliance with the HIPAA Security Rule. The following types of questions will be used to acquire this information:
* During the last 12 months, has their subcontractor conducted a HIPAA security risk assessment for the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information?
* Has their subcontractor signed a Business Associate contract that complies with the 2013 HIPAA Final Rule with the business associate?
* Does their subcontractor have written policies and procedures that address and comply with the HIPAA Breach Notification Rule and the Security Rule’s administrative, technical, organizational and physical safeguard requirements?
* Has their subcontractor implemented a HIPAA-compliant security awareness and training program and trained all employees and contractors?
* Does their subcontractor’s IT services meet HIPAA compliant security standards for protecting electronic protected health information?
* Retain documentation (e.g. business associate and subcontractor due diligence findings, business associate contracts, contract review log) of the practices in place as evidence of compliance.

**Location of supporting documentation:** If so, identify the document and location it is stored here.

## REVISION HISTORY

| Revision | Date | Initiator | Nature of Change |
| --- | --- | --- | --- |
| 0 |  |  | Initial draft |
| 1 |  |  |  |