

164.314: Organizational Requirements

§164.314(a)(1): Standard: Business associate contracts or other arrangements. The contract or other arrangement required by §164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.

This requires implementation of the following HIPAA specific “Implementation Specifications”:

- **§164.314(a)(2)(i):** Business associate contracts. The contract must provide that the business associate will--
- **§164.314(a)(2)(i)(A):** Comply with the applicable requirements of this subpart;
- **§164.314(a)(2)(i)(B):** In accordance with §164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and
- **§164.314(a)(2)(i)(C):** Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.
- **§164.314(a)(2)(ii):** Other arrangements. The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of §164.504(e)(3).
- **§164.314(a)(2)(iii):** Business associate contracts with subcontractors. The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by §164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

Thus, please answer the following questions regarding the aforementioned HIPAA specific “Implementation Specifications”:

1. *Are you identified as a Covered Entity (CE) for purposes of HIPAA compliance and do you have documented Business Associates contracts (Business Associates Agreements (BAA) in place with all BA’s? (Note: If you are not identified as a CE, then proceed to question 3).*

Answer:

2. *Do your Business Associates have contracts in place (Business Associates Agreements (BAA) with all their respective BA’s, (i.e., their subcontractors)?*

Answer:

3. *Are you identified as a Business Associate (BA) for purposes of HIPAA compliance and do you have documented Business Associates contracts (Business Associates Agreements (BAA) in place with all of your respective BA’s (i.e., your subcontractors)?*

Answer:

4. *Has your organization suffered any type of data breach within that last 36 months – and if so – did it result in the compromise of Protected Health Information (PHI)?*

Answer: