45 CFR 164.314: Organizational Requirements

A. *Standard:* Business associate contracts or other arrangements.

1. The contract or other arrangement between the covered entity and its business associate required by § 164.308(B) must meet the requirements of paragraph (A-2) or (A-2-a) of this section, as applicable.

2. *A covered entity is not in compliance with the standards in* by § 164.502(E) and paragraph (A) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful-

a. Terminated the contract or arrangement, if feasible; or

b. If termination is not feasible, reported the problem to the Secretary.

3. *Implementation specifications* (Required)

a. Business associate contracts. The contract between a covered entity and a business associate must provide that the business associate will-

- Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart;

- Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;

- Report to the covered entity any security incident of which it becomes aware;

- Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

4. Other arrangements.

a. When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (A-1) of this section, if-

- It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (A-2) of this section; or

- Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (A-2) of this section.

b. If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in § 160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (A-2) of this section, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph

(A-2-a) of this section and documents the attempt and the reasons that these assurances cannot be obtained.

c. The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity, as required by paragraph (A-2) of this section if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

B. **1.** *Standard:* Requirements for group health plans. Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(F), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.

a. *Implementation specifications* (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-

- Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan;

- Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;

- Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and

- Report to the group health plan any security incident of which it becomes aware.