

**THE UNIVERSITY OF TEXAS SYSTEM ADMINISTRATION
HIPAA PRIVACY MANUAL**

Section 6.1: Contracts With Business Associates Involving Office of Employment Benefits PHI	Page: 1 of 3
Effective Date: September 23, 2013	

POLICY

A Business Associate is a person or entity, other than a member of the workforce of a Covered Entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. System shall require any Business Associate of OEB other than a System Office within the Health Care Component to agree by written agreement to certain restrictions and duties with respect to PHI that the Business Associate creates, collects or holds on behalf of System in its capacity as a Covered Entity.

6.1(1) Identifying Business Associates

System shall review existing Self-funded Group Health Plan-related contracts that involve Use or Disclosure of PHI in order to determine whether such contracts need to be amended to include Business Associate agreement provisions. Contracts between Business Associates and Business Associates that are subcontractors are subject to these same requirements. Prior to entering into any new agreement with another entity concerning such services or activities, System shall determine whether the entity is a Business Associate as a result of such services or activities.

Business Associates include persons or entities who have periodic contact with PHI (e.g., outside auditors), or that have contact with PHI or (e.g., vendors providing software or hosting services) that require the vendor to persistently store PHI even if the vendor does not access the PHI.

6.1(2) Contracting with Business Associates

If a Business Associate creates, receives, Uses, or Discloses OEB PHI, System shall require the Business Associate to enter into a written contract or other written agreement with System that:

- a. Establishes the Business Associate's permitted and required Uses and Disclosures of System PHI;
- b. Provides that the Business Associate will not further Use or Disclosure PHI other than as permitted by the contract or a permitted by law;

- c. Provides that the Business Associate shall use appropriate safeguards, including implementing requirements of the HIPAA Security Rule with regard to electronic PHI;
- d. Provides that the Business Associate shall report to OEB any Use or Disclosure of EGI PHI not provided for by the agreement of which it becomes aware;
- e. require the Business Associate to disclose protected health information as specified in its contract to satisfy System's obligation with respect to individuals' requests for copies of their PHI, as well as make available PHI for amendments (and incorporate any amendments, if required) and accountings;
- f. to the extent the Business Associate is to carry out a System's obligation under the Privacy Rule, require the Business Associate to comply with the requirements applicable to the obligation;
- g. require the Business Associate to make available to the Secretary its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity for purposes of determining the covered entity's compliance with the HIPAA Privacy Rule;
- h. at termination of the contract, if feasible, require the Business Associate to return or destroy all protected health information received from, or created or received by the Business Associate on behalf of, System;
- i. require the Business Associate to ensure that any subcontractors it may engage on its behalf that will have access to protected health information agree to the same restrictions and conditions that apply to the Business Associate with respect to such information; and
- j. authorize termination of the contract by System if the Business Associate violates a material term of the contract.

Notwithstanding the foregoing, if an entity is required by law to perform an activity or provide a service, and the entity qualifies as a Business Associate solely because of such legally required activities or services, System must require the entity to enter into a written agreement as described above.

In any case where the services are to be provided by another governmental entity, this section can be satisfied by a memorandum of understanding with the other government entity that contains terms that accomplish the objectives of the HIPAA Privacy Standards that relate to Business Associate Agreements.

6.1(3) Monitoring Business Associates

If System learns that a Business Associate has materially violated one or more of the written agreement's provisions described in subsection 6.1(2) of this Section, System shall take reasonable steps to end the violation and mitigate the violation's harmful effects in accordance with Section 8.4 of this Manual. If System's steps to end the violation and mitigate its effects are unsuccessful, System shall terminate the contract or arrangement with the Business Associate or, if the Privacy Officer determines that such termination is not feasible, report the problem to the Secretary.

6.1(4) Documentation of Business Associates.

System shall retain any written agreement with a Business Associate, or any other set of written provisions intended to comply with this Section. Such documentation shall be retained in accordance with Section 9.2 of this Manual.

REFERENCES/CITATIONS

45 C.F.R. §§ 164.502(e), 164.504(e)