


<b>Name of Policy:</b> Business associate agreement  <b>Policy Number:</b> 3364-90-13  <b>Approving Officer:</b> President  <b>Responsible Agent:</b> Privacy Officer and Director of Health Information Management  <b>Scope:</b> Hybrid and affiliated covered entity of University of Toledo		  <b>Effective date:</b> September 13, 2023  <b>Original effective date:</b> November 15, 2010	
<b>Keywords:</b>			
	New policy		Minor/technical revision of existing policy
	Major revision of existing policy	X	Reaffirmation of existing policy

(A) Policy statement

The hybrid and affiliated covered entities as defined below will comply with the Health Insurance and Portability Act of 1996 (HIPAA) in regards to its use or disclosure of protected health information (PHI).

(B) Purpose of policy

The purpose of this policy is to ensure compliance with business associate requirements as defined in the Privacy Act under HIPAA regulations in section 164.504(e)(2) or (e)(3) with regards to the use and disclosure of PHI under CFR section 164.502(e)(2).

(C) Procedure

- (1) A business associate addendum/agreement must be fully-executed between the university and all business associates as defined below, that perform any function or activity as defined below, on behalf of the university involving the use or disclosure of PHI where the business associate is *not*

considered a workforce member of a designated healthcare component of the university for purposes of HIPAA.

- (a) It is the responsibility of the university department with the business associate relationship to ensure that an appropriate business associate agreement is fully executed between the university and the business associate prior to the business associate receiving or gaining any access to PHI.
  - (b) The business associate agreement must be approved by the office of legal affairs in compliance with the University's policy 3364-10-14 Contract review and approval process.
  - (c) The business associate agreement signature authority is incorporated into the university's policy 3364-40-08 Delegation of signature authority for documents that bind the university.
- (2) Business associate agreements will comply with the Privacy Act under HIPAA regulations in section 164.504(e)(2) and (e) (3) with regards to the use and disclosure of protected health information as outlined under CFR section 164.502(e)(2). Business associate agreements and their applicable service agreements will:
- (a) Establish the permitted and required use and disclosure of PHI by the business associate. The contract may not authorize the business associate to use or further disclose PHI that would violate the Privacy Act. The contract may permit the business associate to use and disclose PHI for the proper management and administration of the business associate as permitted by the contract and in accordance with the conditions set forth at 45 C.F.R. 164.504(e) and (e)(4) as required by law.
  - (b) Obligate the business associate to:
    - (i) Use appropriate safeguards to prevent unauthorized use or disclosure of PHI other than as provided under the applicable agreement.
    - (ii) Make available the information required to provide an accounting of disclosure in accordance with section 164.528.
    - (iii) Make access PHI available in accordance with section 164.524.
    - (iv) Make available to the covered entity any information the business associate or its agents or subcontractors maintain in

- designated record sets on behalf of the covered entity for inspection and to respond to a request for the same.
- (v) Make available the PHI for amendments and incorporate any amendments to the PHI in accordance with section 164.526.
  - (vi) Report to the covered entity any unauthorized use or disclosure of which it becomes aware.
  - (vii) Make available for inspection its internal practices, books and records relating to the use and disclosure of PHI received from, created or received by the business associate on behalf of the covered entity to the secretary of health and human services for purposes of determining the covered entity's compliance.
  - (viii) Ensure that any agents, including subcontractors, to whom it provides PHI received from, or created or received by the business associates on behalf of the covered entity, agrees to the same restrictions and conditions that apply to the business associate with respect to such information.
- (3) Covered entity will immediately terminate the applicable agreement with the business associate upon a determination by the covered entity in its sole discretion that the business associate has breached the terms of the business associate agreement. If a covered entity becomes aware of a pattern of activity or practice by a business associate that constitutes a material breach, it must take reasonable steps to remedy the situation. If such steps are not successful, terminate the agreement or arrangement; or if termination is not feasible, report the problem to secretary of health and human services.
- (4) At termination of the agreement, the business associate will return or destroy all PHI received from, created or received by the business associate on behalf of the covered entity that the business associate still maintains in any form. The business associate will retain no copies of such information. If such return or destruction is not feasible, extend the protection of the agreement to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.
- (5) Exceptions
- (a) Business associate requirements do not apply to disclosures by a covered entity to a healthcare provider for treatment purposes; for example, PHI exchanged between a hospital and physicians with admitting privileges. However, a covered entity may be a business

associate of another covered entity for non-treatment functions and activities, and will be bound by the contractual assurances it gave as part of that relationship.

- (b) The business associate requirements do *not* apply to:
  - (i) Disclosures to the plan sponsor by a group health plan, or a health insurance issuer or health maintenance organization (HMO) with respect to a group health plan (if other requirements are met); nor to
  - (ii) The collection and sharing of PHI by a health plan that is a public benefits program and an agency other than the agency administering the health plan, in order to determine eligibility or enrollment.

(6) Other arrangements

- (a) If the covered entity and the business associate are both governmental entities, the covered entity may disclose PHI to the business associate and may allow the business associate to create or receive PHI on its behalf only if the covered entity executes a satisfactory contract or other written agreement (such as a memorandum of understanding) that accomplishes the objectives outlined in (C)(2)(a) and (C)(2)(b), above.
- (b) If the business associate is required by law to perform a function or activity on behalf of the covered entity or to provide a service described in the definition of business associate to a covered entity, the covered entity may disclose PHI to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements as listed above, provided that good faith attempts to obtain satisfactory assurances and failed attempts to document the reason that such assurances cannot be obtained. The termination clause may be omitted from the arrangements if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(7) Other requirements for agreement and other arrangements

The agreement or other arrangements between the covered entity and the business associate may permit the business associate to use the information

received by the business associate in its capacity as a business associate to the covered entity, if necessary:

- (a) For the proper management and administration of the business associate; or
  - (b) To carry out the legal responsibilities of the business associate.
- (8) The agreement or other arrangements between the covered entity and the business associate may permit the business associate to disclose the information received by the business associate in its capacity as a business associate if the
- (a) Disclosure is required by law, or
  - (b) The business associate obtains reasonable assurance from the person to whom the information is disclosed that it will be held confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and the person notified the business associate of any instances of which it is aware in which confidentiality of the information has been breached.

(D) Definitions

- (1) Business Associate. HIPAA defines a business associate as:
  - (a) an individual or corporate “person” that: creates, receives, maintains, or transmits PHI on behalf of the covered entity any function or activity involving the use or disclosure of protected health information; and
  - (b) is *not* a member of the covered entity's workforce and part of the designated healthcare component.
- (2) Function or activity relates to legal, actuarial, accounting, consulting, data processing, management, administrative, accreditation, financial services and anything else for which a covered entity might contract out are included, if access to PHI is involved.
- (3) Healthcare component is defined in university policy 3364-15-01 Confidential patient information under HIPAA as “... the entire health science campus in addition to certain departments or units on the main campus of the university as healthcare components which are covered entities for

purposes of HIPAA compliance”. The privacy officer maintains the list of the university healthcare components. A list of designated healthcare components can be obtained by contacting the privacy officer.

<p><b>Approved by:</b></p> <hr/> <p>Gregory Postel, MD President</p> <p><b>Date:</b> September 13, 2023</p> <p><b>Review/revision completed by:</b></p> <ul style="list-style-type: none"> <li>• <i>Privacy and Security Committee</i></li> <li>• <i>Senior Leadership Team</i></li> </ul>	<p><b>Policies superseded by this policy:</b></p> <ul style="list-style-type: none"> <li>• <i>None</i></li> </ul> <p><b>Original effective date:</b> <i>November 15, 2010</i></p> <p><b>Review/revision date:</b> <i>March 1, 2014</i> <i>June 21, 2016</i> <i>October 16, 2017</i> <i>October 6, 2020</i> <i>September 13, 2023</i></p> <p><b>Next review date:</b> <i>September 13, 2026</i></p>
--	--