3364-90-13 Business associate agreement.

(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 C.F.R. 164.504(e) (2) or (e) (3) with regards to the use and disclosure of PHI under C.F.R. 164.502(e) (2).

(C) Procedure

(1) A business associate addendum/agreement "BAA" 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 "BA" relationship to ensure that an appropriate BAA is fully executed between the university and the BA prior to the BA receiving or gaining any access to PHI.

(b) The BAA must be approved by the office of legal affairs in compliance with rule 3364-10-14 of the Administrative Code (contract review and approval process).

(c) BAA signature authority is incorporated into rule 3364-40-08 of the Administrative Code (delegation of signature authority for documents that bind the university).

(2) BAAs will comply with the privacy act under HIPAA regulations in C.F.R.164.504 (e) (2) and (e) (3) with regards to the use and

disclosure of protected health information as outlined under C.F.R. 164.502(e) (2). BAAs and their applicable service agreements will:

(a) Establish the permitted and required use and disclosure of PHI by the BA. The contract may not authorize the BA to use or further disclose PHI that would violate the privacy act. The contract may permit the BA to use and disclose PHI for the proper management and administration of the BA 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 BA 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 C.F.R.164.528.

(iii) Make access PHI available in accordance with C.F.R. 164.524.

(iv) Make available to the covered entity any information the BA 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 C.F.R. 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 BA 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 BA on behalf of the covered entity, agrees to the same restrictions and conditions that apply to the BA with respect to such information.

(3) Covered entity will immediately terminate the applicable agreement with the BA upon a determination by the covered entity in its sole discretion that the BA has breached the terms of the BAA. If a covered entity becomes aware of a pattern of activity or practice by a BA 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 BA will return or destroy all PHI received from, created or received by the BA on behalf of the covered entity that the BA still maintains in any form. The BA 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) BA 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 BA 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 BA are both governmental entities, the covered entity may disclose PHI to the BA and may allow the BA 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 paragraph (C)(2)(a) and (b) of this rule.

(b) If the BA 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 BA to a covered entity, the covered entity may disclose PHI to the BA 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 it's BA.

(7) Other requirements for agreement and other arrangements

(a) The agreement or other arrangements between the covered entity and the BA may permit the BA to use the information received by the BA in its capacity as a BA to the covered entity, if necessary:

(i) For the proper management and administration of the BA; or

(ii) To carry out the legal responsibilities of the BA.

(8) The agreement or other arrangements between the covered entity and the BA may permit the BA to disclose the information received by the BA in its capacity as a BA if the:

(a) Disclosure is required by law, or

(b) The BA 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 BA of any instances of which it is aware in which confidentiality of the information has been breached.

(D) Definitions

(1) Business associate or "BA:" 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 confidential patient information under rule 3364-15-01 of the Administrative Code (HIPAA organizational structure and administrative responsibilities) 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.

Effective: 7/9/2018

CERTIFIED ELECTRONICALLY

Certification

06/29/2018

Date

Promulgated Under:	111.15
Statutory Authority:	3364
Rule Amplifies:	3364