TITLE

HIPAA Business Associate Agreements

PURPOSE

In accordance with 45 CFR §§ 164.502(e), 164.504(e), 164.308 and 164.314, this procedure provides the following guidance to The University of Arizona (UA):

- Identifying Business Associates (BAs);
- Ensuring that the UA Covered Components enter into written Business Associate Agreements (BAAs) prior to allowing BAs to access, use, disclose or maintain Protected Health Information (PHI) for or on behalf of UA; and
- Ensuring that UA enters into written Business Associate Agreements (BAAs) prior to conducting work for or on behalf of a Covered Entity (CE).

Please note: Human subject research at UA is generally not considered part of the "Covered Component," therefore, Business Associate Agreements are generally not appropriate when a researcher seeks to use or disclose Individually Identifiable Health Information. See the University of Arizona Privacy, Security and Breach Notification Policy (2013) for additional information about UA's status as a Hybrid Entity.

REVIEW/REVISIONS

- 06/2015

REFERENCES AND RELATED FORMS

- Capitalized terms are defined in HIPAA Privacy Program Guidance (Definitions of Key Words) and 45 CFR Parts 160 and 164
- Please contact the HIPAA Privacy Program or Contract & Research Support (CRS) for a template Business Associate Agreement or if you receive a Business Associate Agreement (caution: BAAs are often included in Service Agreements).

PROCEDURES

Prior to contracting with any outside person, whether an individual or an entity, it is the responsibility of the using department or individual to contact the HIPAA Privacy Program to determine whether the outside entity or person qualifies as a Business Associate.

1. Procedures: If an outside person provides services requiring the use or disclosure of PHI and meets the definition of a BA, and the outside person has no known written BAA, UA personnel shall notify the HIPAA Privacy Program of the need for a BAA.
    A. If the determination is made that either UA or the outside person or

entity is a Business Associate, both parties are required to enter into a written Business Associate Agreement.

2. Role of the HIPAA Privacy Program:
    A. The HIPAA Privacy Program should periodically reevaluate the list of BAs to determine who is using or disclosing PHI in order to assess, to the extent feasible or required:
        i. Whether the list is complete and current;
        ii. Whether the UA department, clinic, or individual has acted in compliance with the agreement; and
        iii. Whether the BAs of UA have acted in compliance with the agreement.
    B. The HIPAA Privacy Program will coordinate relevant (IT) Security Rule compliance with the Information Security Office in order to identify systems covered by the BAA.

3. Business Associate Agreements: The BAA must establish the permitted and required uses and disclosures of PHI by the Business Associate, and may:
    A. Permit the Business Associate to use and disclose PHI for the proper management and administration of the Business Associate;
    B. Permit the Business Associate to provide data aggregation services relating to the health care operations of the CE;
    C. Provide that the Business Associate will:
        i. Not use or further disclose the information other than as permitted or required by the contract or as required by law;
        ii. Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;
        iii. Report to the CE any use or disclosure of the information not provided for by its contract of which it becomes aware;
        iv. Ensure that any agents, including a subcontractor, to whom it provides PHI received from, or created or received by the BA on behalf of, the CE agrees to the same restrictions and conditions that apply to the BA with respect to such information;
        v. Make available PHI in accordance with 45 CFR § 164.524;
        vi. Make available PHI for amendment and incorporate any amendments to PHI;
        vii. Make available the information required to provide an Accounting

of Disclosures;

viii. Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the Business Associate on behalf of, the CE available to the HHS Secretary for purposes of determining the CEs compliance; and

ix. At termination of the contract, if feasible, return or destroy all PHI received from, or created or received by the Business Associate on behalf of, the CE that the Business Associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

4. Business Associate Agreement Implementation
   A. Contracting & Research Services (CRS) will process all BAAs.
   B. Prior to the agreement being fully executed, CRS will consult with UA HIPAA Privacy Program for review and approval of the BAA to ensure compliance with HIPAA requirements.
   C. The HIPAA Privacy Officer will sign the completed BAA as an attestation.