University of Colorado
Denver | Anschutz Medical Campus

Office of Regulatory Compliance

13001 E. 17th Place, Suite W1124
Mail Stop F497
Aurora, CO 80045
Main Office: 303-724-1010
Main Fax: 303-724-1019

HIPAA Policy 8.1

Title:	**Privacy Practices re: Business Associates**
Source:	**Office of Regulatory Compliance**
Prepared by:	**Assistant Vice Chancellor for Regulatory Affairs**
Approved by:	**Vice Chancellor for Research**
Effective Date:	**July 1, 2013**
Replaces:	**02/26/03**
Applies:	**All UCD campuses**

Introduction

Purpose

To Define:

1. When a covered entity may or may not disclose PHI to a business associate or governmental entity, and when a business associate may create or receive PHI on its behalf. Satisfactory assurances must be provided that the business associate or governmental entity will appropriately safeguard the information.

2. The requirements of contracts or other arrangements between the covered entity and the business associate or governmental entity.

3. Steps the covered entity may take if it discovers that the business associate or governmental entity has violated the contract.

Reference

45 C.F.R. § 164.502(e) and § 164.504(e)

Applicability

This policy is to ensure that privacy rights pertaining to the use or disclosure of PHI are maintained with respect to business associates, including governmental entities.

Policy

The UCD shall ensure that the use or disclosure of PHI to business associates, including governmental entities, shall be described in a written agreement and that PHI is protected by that agreement. In addition, if the agreement has not been reviewed by the UCD Office of Grants and Contracts, University Counsel, Procurement Service Center and/or Technology Transfer (as applicable), it is void. If anyone from UCD becomes aware of violations of these privacy rights by business associates, including governmental entities, it is his or her responsibility to take reasonable steps to end the violation or terminate the passage of PHI to the business associate.

Procedures

The UCD has an established communication mechanism and guidelines for the purpose of ensuring that privacy rights pertaining to the use and disclosure of PHI by business associates, including governmental entities, are maintained.

1. Under this policy, UCD may disclose PHI to a business associate and may allow a business associate, to create or receive PHI on its behalf, as long as UCD obtains satisfactory assurance that the business associate will appropriately safeguard the information. This standard does not apply:

    a. to disclosures to a health care provider concerning treatment of an individual;

    b. to disclosures by a group health plan or health insurance issuer or HMO with respect to a group health plan to the plan sponsor.

    c. to uses and disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the PHI used is to determine enrollment or eligibility in the health plan is collected by an agency other than the agency administering the health plan, and such activity is authorized by law, with respect to the collection and sharing of IIHI for the performance of such functions by the health plan and the agency administering the health plan.

2. UCD shall assure in writing (e.g. in a written contract or other written agreement) that the business associate will appropriately safeguard PHI. The contract or agreement shall include:

    a. The permitted and required uses and disclosures of PHI by the business associate;

    b. The contract may permit the business associate to provide data aggregation services relating to the health care operations of the UCD;

c. The contract may permit the business associate to use and disclose PHI for the proper management and administration of the business associate, or to carry out its legal responsibilities;

d. That the business associate will:

i. Not use or further disclose the PHI other than as permitted or required by the contract or as required by law;

ii. Use appropriate safeguards to prevent use or disclosure of PHI other than as provided by the contract;

iii. Report to the UCD any use or disclosure of PHI not provided for by the contract, of which it becomes aware;

iv. Ensure that any agents, including subcontractors, to whom the business associate provides PHI received from the UCD, agrees to the same restrictions and conditions that apply to the business associate;

v. Make available PHI in accordance with UCD policies on Access of Individuals to PHI and Accounting of Disclosures;

vi. Make available PHI for amendments and incorporate amendments to PHI;

vii. Make available to the Secretary of HHS internal practices, books and records relating to use and disclosure of PHI, for the purpose of determining compliance by the UCD;

viii. At termination of the contract, if feasible, return all PHI to UCD, or destroy all PHI;

ix. Authorize termination of the contract by UCD if the UCD determines that the business associate has violated a material term of the contract or agreement.

3. If UCD becomes aware of a pattern of activity or practice by the business associate that constitutes a material breach or violation of the business associate's obligation and/or of HIPAA, UCD shall take reasonable steps to comply with this policy and other UCD HIPAA policies. These steps include:

a. Allowing the business associate to cure the breach or end the violation;

b. Termination of the contract or agreement, if feasible;

c. If termination is not feasible, reporting the problem to the Secretary of HHS.

4. The contract may not authorize the business associate to use or further disclose the PHI in a manner that would violate HIPAA, if done by the UCD.

5. Whenever possible, UCD will require the Business Associate to sign the UCD Business Associate template agreement.

6. All BAAs submitted to the ORC for review must include a completed Data Management and Security Plan (see attached).

BAA DATA MANAGEMENT & SECURITY PLAN

BAA #	(to be filled in by ORC)
COMIRB #	
Data stored electronically? (Y/N)	
Stored on secure server? (Y/N)	
Describe the system/application used for collection, storage and management of data	
Data on Mobile Device? (Y/N)	
Mobile Device encrypted? (Y/N)	
Describe data access restrictions	
Data accessible via internet? (Y/N)	
E-data transmission method	
Describe data plan for end of study	
Data manager name and contact	