

UNIVERSITY OF FLORIDA  
INFORMATION PRIVACY POLICIES & PROCEDURES  
PRIVACY MANAGEMENT

## HIPAA Organizational Requirements: Business Associates

### □ POLICY

Rev: 05/01/2006

1. Protected health information maintained by the University of Florida may only be disclosed to business associates (BA's) who are contracted specifically to provide support services to the University. Business Associate Agreements (BAA's) permit the disclosure of PHI to such contractors and holds the contractor accountable for safeguarding the PHI.
2. It is the responsibility of each department, division, or operating unit contracting for services with third parties where protected health information will be used or disclosed, to ensure that valid business associate agreements are executed.
3. The University of Florida is responsible if it becomes aware of a pattern of activity or practice of a business associate that constitutes a material breach or violation of the business associate's obligations. The University must take reasonable steps to cure the breach or end the violation, as applicable, and, if such steps are unsuccessful:
  - a. Terminate the contract or arrangement, if feasible; or
  - b. If termination is not feasible, report the problem to the Secretary.

### □ DEFINITIONS

*Business Associate:* A person who, on behalf of a covered entity, performs, or assists in the performance of a function or activity or provides support services, while not a member of the workforce, to the covered entity involving the use or disclosure of individually identifiable health information.

### □ PRIVACY REQUIREMENTS

1. The University is required to assure, to the extent practicable, that any business associate to whom it discloses protected health information manages that information in compliance with federal and state privacy and security regulations.
2. *Business Associate Contracts/Agreements:* Business associate agreements must be in writing and must include terms authorized and approved by the University's Privacy Office for maintaining compliance with federal privacy regulations.
3. *Contents of Contracts:* Contracts between the University of Florida and business associates must:
  - a. Clearly establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of the privacy regulations.
  - b. Define the conditions to which the business associate will adhere, as follows:
    - 1) No use or further disclosure of the information other than as permitted or required by the contract or as required by law;
    - 2) Implementation of appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract, including:
      - a) The BA must immediately report to the University any use or disclosure of the information not provided for by its contract of which it becomes aware.

UNIVERSITY OF FLORIDA  
INFORMATION PRIVACY POLICIES & PROCEDURES  
PRIVACY MANAGEMENT

**HIPAA Organizational Requirements: Business Associates (continued)**

- b) If the BA determines that personally identifiable information was, or is reasonably believed to have been, acquired by an unauthorized person and that the information could be used for fraudulent purposes, the University must be notified immediately, if possible, but no later than 10 days after the determination is made.
  - c) The BA must ensure that any agents, including subcontractors to whom it provides protected health information, agree to the same restrictions and conditions that apply to the business associate with respect to such information;
- 3) Making available protected health information to patients, as required under rights of access and inspection, including:
    - a) Making available protected health information for amendment by the patient, and incorporating any approved amendments into protected health information maintained by the business associate;
    - b) Making available the information required to provide an accounting of disclosures;
  - 4) Making available its internal practices, books, and records, concerning the use and disclosure of protected health information, to the Secretary for purposes of determining the University's compliance with the privacy regulations; and
  - 5) At termination of the contract, if feasible, return or destruction of all protected health information that the business associate still maintains in any form, retaining no copies of such information or, if return or destruction is not feasible, extending the protections of the contract to the retained information and limiting further uses and disclosures to those purposes that make the return or destruction of the information infeasible.
  - 6) Required implementation of administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic protected health information that it creates, receives, maintains or transmits on behalf of the covered entity;
  - 7) Ensuring that any agent, including a subcontractor, to whom the business associate provides protected health information, agrees to implement reasonable and appropriate safeguards to protect it.
- c. Authorize termination of the contract by the University of Florida, if at any time the University determines that a business associate has violated a material term or obligation under the agreement relating to HIPAA compliance.
    - 1) The department that is party to the agreement and/or the University Privacy Officer shall be notified and shall seek to immediately remedy the breach or, if that is not possible, to alter or terminate the agreement.
    - 2) The University may also report violations to the Secretary of the Department of Health and Human Services.

UNIVERSITY OF FLORIDA  
INFORMATION PRIVACY POLICIES & PROCEDURES  
PRIVACY MANAGEMENT

## **HIPAA Organizational Requirements: Business Associates (continued)**

3. *Purchase Orders:* Purchases with certain accounting codes (see Appendix C in this manual) have been identified as potential opportunities for exposing PHI. Where no contract exists, but HIPAA-related implications may apply for a general purchase, the Purchase Order will include the following statement, in lieu of a contract:

*VENDOR acknowledges that VENDOR may have access to protected health Information (PHI) in various formats. VENDOR agrees to comply with all laws and policies covering security and confidentiality of PHI and to cooperate with the University of Florida's monitoring of such compliance. VENDOR shall ensure that it will maintain all PHI in a secure and confidential fashion and that no PHI is disclosed to any third party except as permitted by law. VENDOR shall not disclose any PHI without first obtaining consent from the person to whom the record pertains or that person's legal representative.*

### **□ PROCEDURES**

1. Identify the type of client for which the Business Associate Agreement (BAA) is to be written:
  - a. Refer all Clinical Business Associate Agreements to the Office of Contracts and Related Services.
  - b. Refer all non-Clinical Business Associate Agreements to the UF Purchasing Office.
2. Provide the contract office or the purchasing office with the information necessary to complete the appropriate Business Associate Agreement template, including all required privacy and security safeguards.
3. When BAA template language is materially changed, the Privacy Office must approve the changes. Legal review of a changed agreement may also be required.

### **□ REFERENCES**

HIPAA Regulations: 45CFR §160.103 (Definitions), §165.504 (Organizational Requirements)  
Florida Statute: 817.568 and 817.5681 (Criminal Use of Personal Identification Information)

**EXHIBITS:** Appendix C: Accounting Codes for Purchase Orders