



## UNIVERSITY POLICY

**SUBJECT:** CORPORATE COMPLIANCE AND PRIVACY      **TITLE:** DISCLOSURES OF PERSONALLY IDENTIFIABLE HEALTH INFORMATION TO BUSINESS ASSOCIATES

**CODING:** 00-01-15-40:00      **ADOPTED:** 4/14/03      **AMENDED:** 03/24/05

---

### I. PURPOSE

To assure compliance with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) in relation to disclosures of Protected Health Information (PHI) and to entering into contracts with business associates.

### II. ACCOUNTABILITY

Under the direction of the President, the Deans, Senior Vice President for Administration and Finance, Senior Vice President for Academic Affairs, Vice President for Finance and Treasurer, Vice President for Legal Management and Presidents/CEOs of the Healthcare Units shall ensure compliance with this policy.

### III. APPLICABILITY

This policy shall apply to disclosures to business associates of health information that is generated during provisions of health care to patients in any of the University's patient care units, patient care centers of faculty practices as well as Human Subjects research under the auspices of the University or by any of its agents in all UMDNJ Schools, Units, Departments and University owned or operated facilities.

### IV. DEFINITIONS

- A. Protected Health Information (PHI) - For a full explanation of what constitutes protected health information, see University policy 00-01-15-15:00, Uses and Disclosures of Health Information With and Without an Authorization.
- B. Business Associates - A person other than in the capacity of a member of the workforce that on behalf of UMDNJ, its units, or any organized health care arrangement in which it participates, performs or assists in the performance of:
1. a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management and repricing; or
  2. any other function or activity regulated by HIPAA regulations; or
  3. provides legal, actuarial, accounting, auditing, consulting, data aggregation (as defined in CFR § 164.501), management, administrative, accreditation, or financial services to or for UMDNJ and/or its units, or to or for an organized health care arrangement in which UMDNJ and or its units participate, where the provision of the service involves the

disclosure of individually identifiable health information from such entities or arrangement, or from another business associate of such entities or arrangement, to the person.

- C. Workforce – Faculty, employees, students, volunteers, trainees, and other persons whose conduct, in the performance of work for UMDNJ and/or its units, is under the direct control of such entity(ies), whether or not they are paid by UMDNJ.

## V. REFERENCES

- A. 45 CFR 160.103(a), Code of Federal Regulations, Title 45, Part 164, Section 103, Subpart A, General Administrative Requirements, General Provisions, Definitions
- B. 45 CFR 164.501(e), Code of Federal Regulations, Title 45, Part 164, Section 501, Subpart E, Security and Privacy, Definitions, Privacy of Individually Identifiable Health Information
- C. 45 CFR 164.502(e), Code of Federal Regulations, Title 45, Part 164, Section 502, Subpart E, Security and Privacy, Uses and Disclosures of Protected Health Information: General Rules, Privacy of Individually Identifiable Health Information
- D. 45 CFR 164.504(e), Code of Federal Regulations, Title 45, Part 164, Section 504, Subpart E, Security and Privacy, Uses and Disclosures: Organizational Requirements, Privacy of Individually Identifiable Health Information
- E. 45 CFR 164.532 (d) and (e), Code of Federal Regulations, Title 45, Part 164, Section 532, Subpart E, Security and Privacy, Uses and disclosures: Organizational requirements, Privacy of Individually Identifiable Health Information and (d) Standard: Effect of Prior Contracts or Other Arrangements with Business Associates
- F. Uses and Disclosures of Health Information  
With and Without an Authorization [00-01-15-15:00](#)

The following policy provides additional and related information:

- G. Standards for Privacy of Individually Identifiable Health Information [00-01-15-05:00](#)

## VI. POLICY

- A. Requirements:
  - 1. UMDNJ and/or its units may only allow an individual or entity that is not part of its workforce that provides certain services to UMDNJ and/or its units, or performs a function or activity on its behalf, to create or receive PHI without an authorization if the individual or entity:
    - a. meets the definition of a business associate as described above, and
    - b. enters into a written business associate contract with UMDNJ that meets the elements in 45 CFR 164.504(e) with UMDNJ.
  - 2. To determine whether the person or entity is required to enter into a business associate contract, use the following guidelines with the attached flowchart (EXHIBIT A):
    - a. No contract is needed with members of the workforce as defined in the definition. An independent contractor may be considered a member of the

workforce if UMDNJ exercises supervision and control over the person as it would if the independent contractor was an employee.

- b. A contract is necessary with persons who meet the definition of a business associate. (Since business associates access PHI without obtaining authorizations from the individuals to whom the PHI pertain, it is important that units do not inappropriately classify a person as a business associate and therefore fail to obtain the required authorization).

- i. A business associate is someone who does the following:

- 1. Performs or assists in the performance of a function or activity on behalf of UMDNJ and/or its units including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, repricing, and any other function regulated by 45 CFR 164.504.

- For examples see EXHIBIT B for a list of specific types of persons, entities, and services that may qualify as a business associate provided that they meet all the elements discussed in this policy and procedure (i.e. the person will perform a function on behalf of UMDNJ that is not for the purposes of treatment only, etc).

- 2. Provides legal, auditing, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services for UMDNJ.

- ii. Researchers - This is not a covered function for purposes of a business associate contract.

- iii. Financial Transactions - No business associate agreement is required with a financial institution if it only processes consumer-conducted financial transactions in payment for health care.

- For example, a bank that processes credit or debit card transactions or clears checks for a hospital would not be considered a business associate. Although some PHI of the patient is disclosed to a financial institution in this example, such as the patient's identity and perhaps some health information (e.g., the procedure performed), these facts do not create a business associate relationship because the bank is not acting on behalf of the hospital in performing its functions. The hospital is not in the business of directly processing credit card transactions or cashing checks.

- c. No contract is needed when the person or entity's function or service does not involve the use and disclosure of PHI, and where access to PHI by such persons would be de minimus or incidental, if at all.

- For example, it is not required that UMDNJ enter into a contract with janitorial services because the performance of such services does not involve the use and disclosure of PHI. In this case, where the janitor has contact with PHI incidentally, such disclosure is permitted under the federal privacy laws as an incidental disclosure, provided that reasonable safeguards are in place to prevent such disclosures.

- d. No contract is needed with another healthcare provider when the use or disclosure of the PHI is for treatment purposes.
  - i. If the relationship between the healthcare providers also includes involvement of PHI for operational or payment purposes, then a contract is necessary.

Examples: A hospital enlists the services of another healthcare provider to assist in the hospital's training of medical students. A physician, outside the workforce, serves as a medical director, or provides quality assurance or utilization management services through participation in hospital committees.
  - ii. For the definition and examples of the term treatment, payment, operations see EXHIBIT C.
- e. If it is unclear as to whether the business associate definition has been met or if it is met, whether a contract is necessary, contact Legal Management for assistance. Generally, if it continues to be unclear as to whether there is a business associate relationship, no information should be shared with the person or entity without the patient's authorization.

B. Responsibilities:

- 1. Business associates may only use and disclose PHI to the extent that UMDNJ would be allowed to use and disclose the information. See University policy, 00-01-15-15:00, Uses and Disclosures of Health Information With and Without an Authorization. Only the information minimally necessary to complete the purpose of the service or function may be shared.
- 2. UMDNJ and its units must require business associates to return or destroy all PHI in its possession at the termination of the contract when feasible and permitted by law.
- 3. All UMDNJ units must assure that the individuals and entities identified above agree in writing to the provisions in the attached business associate contract prior to engaging their services or allowing them to encounter any PHI. See EXHIBIT D.
  - a. All departments and units must identify their business associates and have them agree and execute business associate contracts no later than April 14, 2003. UMDNJ and its units must not share any PHI with a business associate without the executed contract after April 14, 2003, with only the following exception in 2(b) below.
  - b. Business associate relationships operating pursuant to a written contract or written other arrangement entered into prior to October 15, 2002 and is not renewed or modified during the period from October 15, 2002 to April 14, 2003 must have the contract executed by the earlier of:
    - i. The date such contract or other written arrangement is renewed or modified on or after April 14, 2003 , or
    - ii. April 14, 2004.

4. For purposes of internal monitoring of compliance with this policy and procedure, all units must maintain a log of all arrangements with parties outside of the workforce accessing business associate arrangements including:
  - a. The name of the business associate.
  - b. The type of services provided to UMDNJ, or the function or activity performed on behalf of UMDNJ.
  - c. The date the business associate provisions were entered into.
  - d. The date the performance or services begin.
  - e. The type of protected health information that will be shared with the business associate.
  - f. Whether any of the protected health information will be shared through electronic means.
5. The above log must be made available to UMDNJ's and the unit's privacy officers upon request.

VII. EXHIBITS

- A. Is a Person or Entity a "Business Associate" and Required to Enter Into a Written Business Associate Contract?
- B. Examples of Potential Business Associates
- C. Treatment, Payment and Health Care Operations
- D. Business Associates Agreement Involving the Access to Protected Health Information

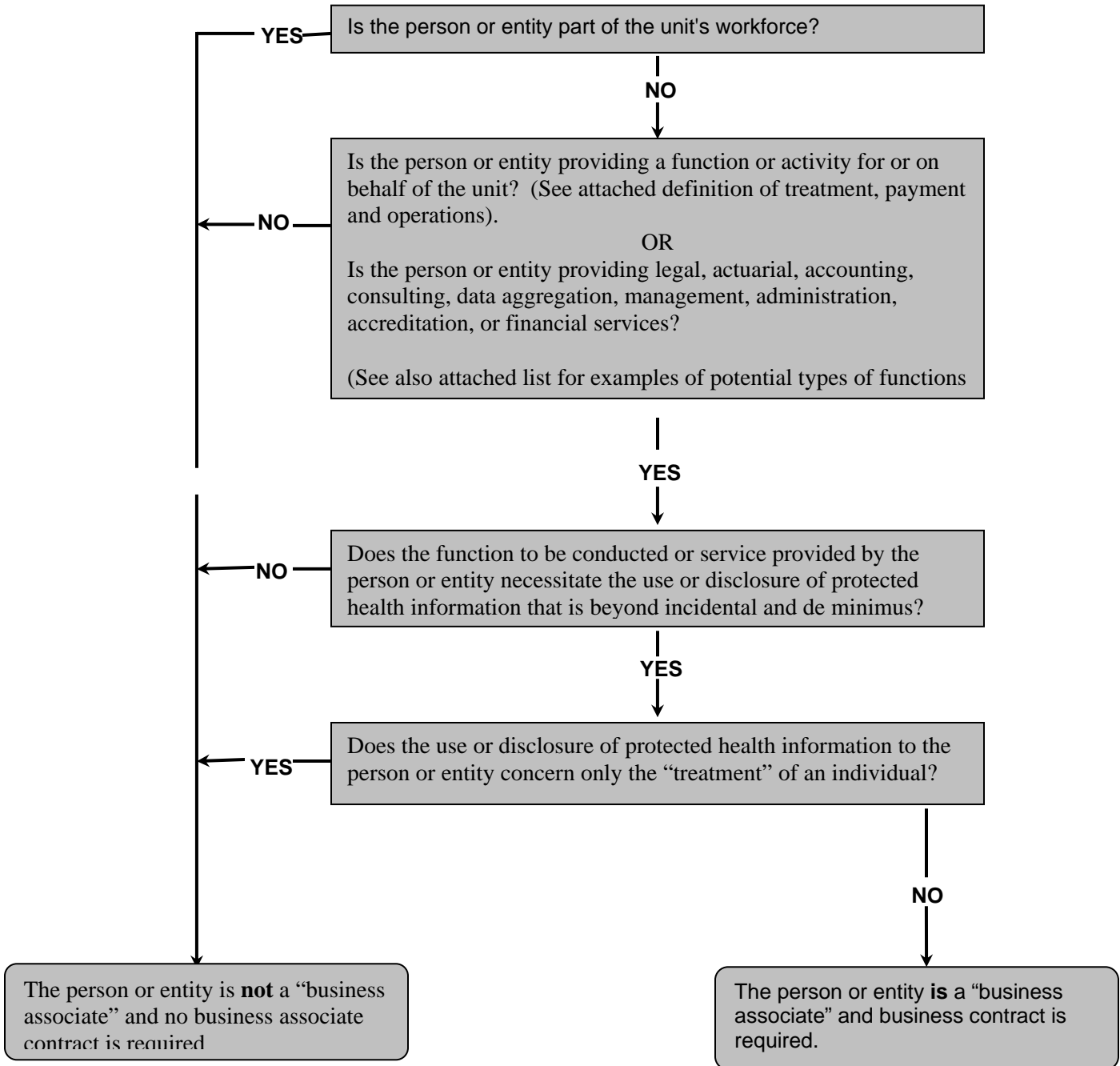
By Direction of the President:

---

Vice President for Legal Management

# EXHIBIT A

## Is a Person or Entity a “Business Associate” and Required to Enter Into a Written Business Associate Contract?



## EXHIBIT B

### Examples of Potential Business Associates

(This is not an all-inclusive list, nor is every arrangement listed necessarily a business associate. Use the attached flowchart and policy and procedure to analyze whether the relationship is a business associate relationship under HIPPA. Contact Legal Management at 2-4705 for assistance in the analysis.)

Accountants
Accounting services and firms
Accreditation services
Actuarial services
Actuarial specialists
Adjudication services
Administrative services
Advertisers
Architects, builders, and contractors
Asset-based lenders to healthcare facilities
Attorneys
Auditors
Billing service companies
Bulk mailing services
Care management programs
Civic groups and other local groups help out on ad hoc basis with patients who are hospitalized for a traumatic event or complicated illness (e.g., Shrine Temples, Ronald McDonald House)
Coding providers and experts
Community health management information systems
Computer maintenance services and companies
Consulting services
Contract Research Organization – An entity used by pharmaceutical and device manufactures to monitor clinical research trials
Copy services
Data aggregation services
Device manufactures
Document storage and destruction vendors
Financial service companies
Government health data systems
Hardware vendors
Healthcare consultants (e.g., risk management, information technology, billing, coding and management)
Hospital associations (National and State)
HVAC vendors
Independent contractors

EXHIBIT B (continued)

Examples of Potential Business Associates

Independent service organizations (ISO) offering clinical/biomedical engineering services
Insurance brokers
Interpreter services (both deaf and foreign language)
Janitorial services; waste disposal and recycling services and companies
Law firms, its staff and employees
Lobbyists
Mailing houses
Maintenance contractors
Management services
Marketing services or firms
Medical equipment testing/ repair services
Medical or Physician associations (National and State)
Medical record moving companies
Medical record storage companies
Medical record transcription services
Medical software vendors
Microfilm conversion providers
Organ and Tissue Banks
Organ procurement organization
Outsourced document shredders
Patient advocates
Pharmaceutical companies
Pharmaceutical manufacturers
Pharmaceutical representatives
Plasma Donor Centers
Printing companies (ID cards and other member materials)
Private health data systems
Professional liability insurance carriers
Recycling services and companies
Software vendors
Sperm Banks
Temporary Staffing Companies
Third-party administrators
Trade associations
Utilization management vendors
Value added networks
Vendors to business associates if involving the disclosure of independently identifiable health information
Waste disposal services and companies

## EXHIBIT C

### Treatment, Payment and Health Care Operations

- A. “Treatment”** - the provision, coordination, or management of health care and related services by one or more health care providers, including:
1. the coordination or management of health care by a health care provider with a third party;
  2. consultation between health care providers relating to a patient; or
  3. the referral of a patient for health care from one health care provider to another.
- B. “Payment”** - the activities undertaken to obtain payment for the provision of healthcare; and relates to the individual to whom health care is provided and includes, but is not limited to:
1. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
  2. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
    - a. Obtaining information about the location of the individual is a routine activity to facilitate the collection of amounts owed and the management of accounts receivable, and, therefore, would constitute a payment activity.
    - b. Debt collection is recognized as a payment activity.
  3. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
  4. Utilization review activities, including pre-certification and pre-authorization of services, concurrent and retrospective review of services; and
  5. Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of reimbursement:
    - a. Name and address;
    - b. Date of Birth;
    - c. Social Security Number;
    - d. Payment history;
    - e. Account number; and
    - f. Name and address of the health care provider and/or health plan.
- C. “Health Care Operations”** - any of the following activities:
1. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contracting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

## EXHIBIT C (continued)

### Treatment, Payment and Health Care Operations

2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care providers, accreditation, certification, licensing, or credentialing activities;
3. Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs;
4. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
5. Business management and general administrative activities of UMDNJ, including, but not limited to:
  - a. Resolution of internal grievances;
  - b. Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity.

## EXHIBIT D

### **Business Associate Agreement** **Involving the Access to Protected Health Information**

The following provisions (Amendment) are added and incorporated into the attached (Name of Agreement) (“Agreement”) entered in between UMDNJ-related entity (“Covered Entity”) and Name of Contracting Party (Business Associate), herein collectively referred to as the “Parties”. Any conflict in the terms of the Agreement and this Amendment shall be governed by the terms of this Amendment.

WHEREAS Covered Entity is the state university of health sciences in New Jersey which maintains and operates (fill in the name of the covered entity);

WHEREAS Business Associate performs \_\_\_\_\_ work which requires it to have access to confidential health information that is considered protected pursuant to federal, state and/or local laws and regulations;

WHEREAS Covered Entity desires to protect the confidentiality and integrity of the information noted above, prevent inappropriate disclosure of such information and comply with all applicable federal, state and/or local laws and regulations governing the use and disclosure of such information;

NOW therefore, the parties agree as follows:

#### 1. Confidentiality and Disclosure of Patient Information.

- A. The Parties to this Agreement agree that Business Associate, its agents and employees may have access to confidential protected health information (“PHI”), including but not limited to demographic information. As used herein, PHI shall mean individually identifiable health information, as defined in 45 CFR § 164.501 which includes health information that (i) identifies an individual (or can be used to form a reasonable basis upon which to identify an individual), (ii) is created or received by a health care provider, health plan, employer, or health care clearinghouse; (iii) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past present, or future payment for the provision of health care to an individual; and (iv) is shared, transmitted or otherwise communicated between Covered Entity and Business Associate (including subcontractors or agents of such parties) in connection with this Agreement.
- B. The Parties to this Agreement agree that Business Associate:
  - a. will not use or further disclose PHI other than as permitted by this Agreement;
  - b. will ensure that all transmissions of PHI are authorized and in accordance with the privacy requirements of the Health Insurance Portability and Accountability Act of 1999, as amended from time to time (“HIPAA”) and will not use or disclose PHI in a manner that violates or would violate HIPAA;
  - c. will implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic Protected Health Information that it creates, receives, maintains or transmits on behalf of the Covered Entity.
  - d. will use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;

## EXHIBIT D (continued)

### **Business Associate Agreement** **Involving the Access to Protected Health Information**

- e. will (i) promptly report to Covered Entity any use or disclosure of PHI not provided for by this Agreement, including but not limited to systems compromises, immediately upon becoming aware of such unauthorized use or disclosure; (ii) will take all necessary steps to prevent and limit any further improper or unauthorized disclosure and misuse of such information; and (iii) indemnify and hold Covered Entity, its directors, officers, agents, and employees harmless from all liabilities, costs and damages arising out of, or in any manner connected with, the disclosure by Business Associate, its employees, agents, or independent contractors; and (iii) permit Covered Entity to investigate any such report and to examine Business Associate's premises, records and premises;
- f. will promptly report to the Covered Entity any security incident of which the Business Associate becomes aware; a security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- g. will ensure that to the extent that the Business Associate it uses one or more agents, including subcontractors, to provide services under this Agreement, such subcontractors or agents who receive or have access to PHI that is received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, will comply with the same restrictions and conditions to which Business Associate is bound by entering into a separate written agreement between Business Associate and its subcontractors to that effect;
- h. will ensure that any agent, including a subcontractor, to whom the Business Associate provides electronic protected health information, agrees to implement reasonable and appropriate safeguard to protect the electronic protected health information.
- i. will, at the request of, and in the time and manner designated by the Covered Entity, provide access to the PHI to the Covered Entity or the individual to whom such PHI relates or his or her authorized representative in order to meet a request by such individual under promptly notify Covered Entity as required by 45 CFR §164.524;
- j. will, at the request of, and in the time and manner designated by the Covered Entity, incorporate any and all amendments or corrections to PHI when notified by Covered Entity that such information is inaccurate or incomplete in accordance with 45 CFR § 164.526;
- k. will, at the request of, and in the time and manner designated by the Covered Entity, provide to the Covered Entity such information as is requested by the Covered Entity, including but not limited to current policies and procedures, operational manuals and/or instructions, and/or employment and/or third party agreements, to permit Covered Entity to respond to a request by an individual for an accounting of the disclosures of the individual's PHI in accordance with 45 CFR 528;
- l. will make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary of Health and Human Services governmental officers and agencies and Covered Entity for purposes of determining compliance with 45 CFR §§ 164.500-534; and
- m. will adhere to the Covered Entity's HIPAA policies and procedures.

## EXHIBIT D (continued)

### **Business Associate Agreement** **Involving the Access to Protected Health Information**

- C. **Termination for violation of disclosure restrictions.** Notwithstanding any other provision of this Agreement, Covered Entity may terminate this Agreement and any related agreements, without penalty if Covered Entity determines that Business Associate has violated a material term of this Agreement's restrictions, safeguards or requirements relating to the proper use and disclosure of PHI. Alternatively, Covered Entity may choose to: (i) provide Business Associate with written notice of the existence of a breach of the terms of this Agreement relating to PHI; and (ii) afford Business Associate an opportunity to cure such breach upon mutually agreeable terms. In the event that mutually agreeable terms cannot be achieved within 10 business days, Business Associate must cure said breach to the satisfaction of the Covered Entity within 10 business days. Covered Entity may immediately terminate this Agreement for Business Associate's failure to cure in the manner set forth in this section.
- D. **Return/Destruction of PHI.** Business Associate agrees that, upon termination of this Agreement for any reason, it will if feasible, return or destroy all PHI maintained in any form (including ensuring the return or destruction of all PHI in the possession of its subcontractors or agents) received from, or created or received by it on behalf of Covered Entity and retain no copies of such information. An authorized representative of Business Associate shall certify in writing to covered Entity, within five (5) days from the date of termination or other expiration of this Agreement, that all PHI has been returned or disposed of as provided above, (including all PHI in the possession of its subcontractors or agents) and that neither Business Associate nor its subcontractors or agents retains any such PHI in any form.
- E. **No Feasible Return/Destruction of PHI.** To the extent that the return or destruction of PHI as provided for in *Section 4* above is not feasible, Business Associate shall extend the precautions of this Agreement to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible. Notwithstanding any other provision of this Agreement to the contrary, Business Associate shall remain bound and shall ensure that the provisions of this Agreement, similarly bind its subcontractors and agents even after termination of this Agreement, until such time as all PHI has been returned or otherwise destroyed as provided in accordance with this section.
- F. **Disclaimer.** Covered Entity makes no warranty or representation that compliance by Business Associate with this Agreement or the HIPAA regulations will be adequate or satisfactory for Business Associate's own purposes or that any information in the possession of Business Associate or control, or transmitted or received by Business Associate, is or will be secure from unauthorized use or disclosure, nor shall Covered Entity be liable to Business Associate for any claim, loss or damage relating to the unauthorized use or disclosure of any information received by Business Associate from Covered Entity or from any other source. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.
- G. **Legal Action.** Business Associate agrees that unauthorized disclosure of PHI may give rise to irreparable injury to the patient or to the owner of such information and accordingly the patient or owner of such information may seek legal remedies against Business Associate. Business Associate further agrees that the remedy at law for any breach by it of the terms of this Agreement shall be inadequate and that the damages resulting from such breach and are not be susceptible to being measured in monetary terms. Accordingly, in the event of a breach or threatened breach by Business Associate of the terms of this Agreement, covered Entity shall be entitled to immediate injunctive relief and may obtain a temporary order restraining any threatened or further breach. Nothing herein shall be construed as prohibiting Business Associate from pursuing any other remedies available to Business Associate for such breach or threatened breach, including recovery of damages from Business Associate. Business Associate further represents that it

EXHIBIT D (continued)

**Business Associate Agreement**  
**Involving the Access to Protected Health Information**

understands and agrees that the provisions of this agreement shall be strictly enforced and construed against it.

- H. **Construction.** This Agreement shall be construed as broadly as necessary to implement and comply with HIPAA. The parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that complies and is consistent with HIPAA.
- I. **Severability.** In the event that any provision of this Agreement violates any applicable statute, ordinance or rule of law in any jurisdiction that governs this Agreement, such provision shall be ineffective to the extent of such violation without invalidating any other provision of this Agreement.
- J. **Authority.** The persons signing below have the right and authority to execute this Agreement for their respective entities and no further approvals are necessary to create a binding agreement.
- K. **Governing Law** This Agreement shall be governed by the laws of the State of New Jersey and shall be construed in accordance therewith.
- L. **Reference:** Code of Federal Regulations, Title 45, Part 160 et seq.

IN WITNESS WHEREOF, the parties have executed this Agreement the day and year first written below.

**Covered Entity**

**Business Associate**

By: \_\_\_\_\_

By: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

**Date:** \_\_\_\_\_

**Date:** \_\_\_\_\_