



UNIVERSITY POLICY

SUBJECT:	CORPORATE COMPLIANCE AND PRIVACY	TITLE:	DISCLOSURES OF PERSONALLY IDENTIFIABLE HEALTH INFORMATION TO BUSINESS ASSOCIATES		
CATEGORY: Check One	Board of Trustees <input type="checkbox"/>	Presidential <input checked="" type="checkbox"/>	Functional <input type="checkbox"/>	School/Unit <input type="checkbox"/>	
Responsible Executive:	Senior Vice President/Chief Ethics & Compliance Officer		Responsible Office:	Privacy & Security	
CODING:	00-01-15-40:00	ADOPTED:	4/14/03	AMENDED:	08/16/11
LAST REVIEWED:					08/16/11

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, Executive Vice President for Academic and Clinical Affairs, Senior Vice President/Chief Ethics & Compliance Officer, Vice President for Finance and Treasurer, Senior Vice President and General Counsel 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):** Protected health information means individually identifiable health information that 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 identifies or could reasonably be used to identify the individual.
1. Except as provided in paragraph two (2) of this definition that is: a) transmitted by electronic media; b) maintained in electronic media; or c) transmitted or maintained in any other form or medium.
 2. Protected health information excludes individually identifiable health information in: a) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; b) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and c) Employment records held by a covered entity in its role as employer.

- 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 re-pricing; 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.
- D. HITECH ACT - Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009 (ARRA) that was enacted on February 17, 2009.

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. Section 13410(d) of the HITECH Act - Breach Notification Interim Final Regulation (74 FR 42740) - August 2009.
- G. Uses and Disclosures of Health Information
With and Without an Authorization [00-01-15-15:00](#)

The following policy provides additional and related information:

- H. 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:
 - a). 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, re-pricing, 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).
 - b). Provides legal, auditing, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, paper recycling, shredder companies, transcription services, record copy services, offsite storage, information technology (IT) services where confidentiality, integrity or availability of ePHI is at risk, including software/hardware support of computing medical devices, and/or application services such email, web or database services 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, waste disposal of sealed materials, or equipment repair because the performance of such services does not involve the use and disclosure of PHI. In this case, any incidental contacts or disclosures 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. Documentation of Business Associate Agreement

UMDNJ and its units will document the satisfactory assurances of protecting health information through a written contract with the business associate that meets the applicable requirements of the Health Insurance and Portability Act (HIPAA), 45 CFR 164.504(e) and 164.308(b).

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.

2. Disclosure of Protected Health Information

UMDNJ and its units may disclose protected health information (PHI) to a business associate and may allow a business associate to create or receive PHI on its behalf, if satisfactory assurances are obtained that the business associate will appropriately safeguard the information.

3. Responsibility of Individuals Authorized to Contract for UMDNJ

Any individual authorized to contract for UMDNJ, or who enters into any form of relationship on behalf of UMDNJ in which PHI is exchanged or in which another entity has access to PHI other than a relationship with another treating provider relating to the treatment of patients, is responsible to obtain satisfactory assurances of protecting health information through the approved business associate contracting process and with the approved business associate contract. Failure to meet this responsibility is subject to disciplinary action up to and including termination and/or dismissal.

4. 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.
5. 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.
6. The above log must be made available to UMDNJ's and the unit's privacy officers upon request.
7. 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, Uses and Disclosures of Health Information With and Without an Authorization, 00-01-15-15:00. Only the information minimally necessary to complete the purpose of the service or function may be shared.

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:

SIGNATURE ON FILE

Senior Vice President/Chief Ethics & Compliance Officer

EXHIBIT A

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

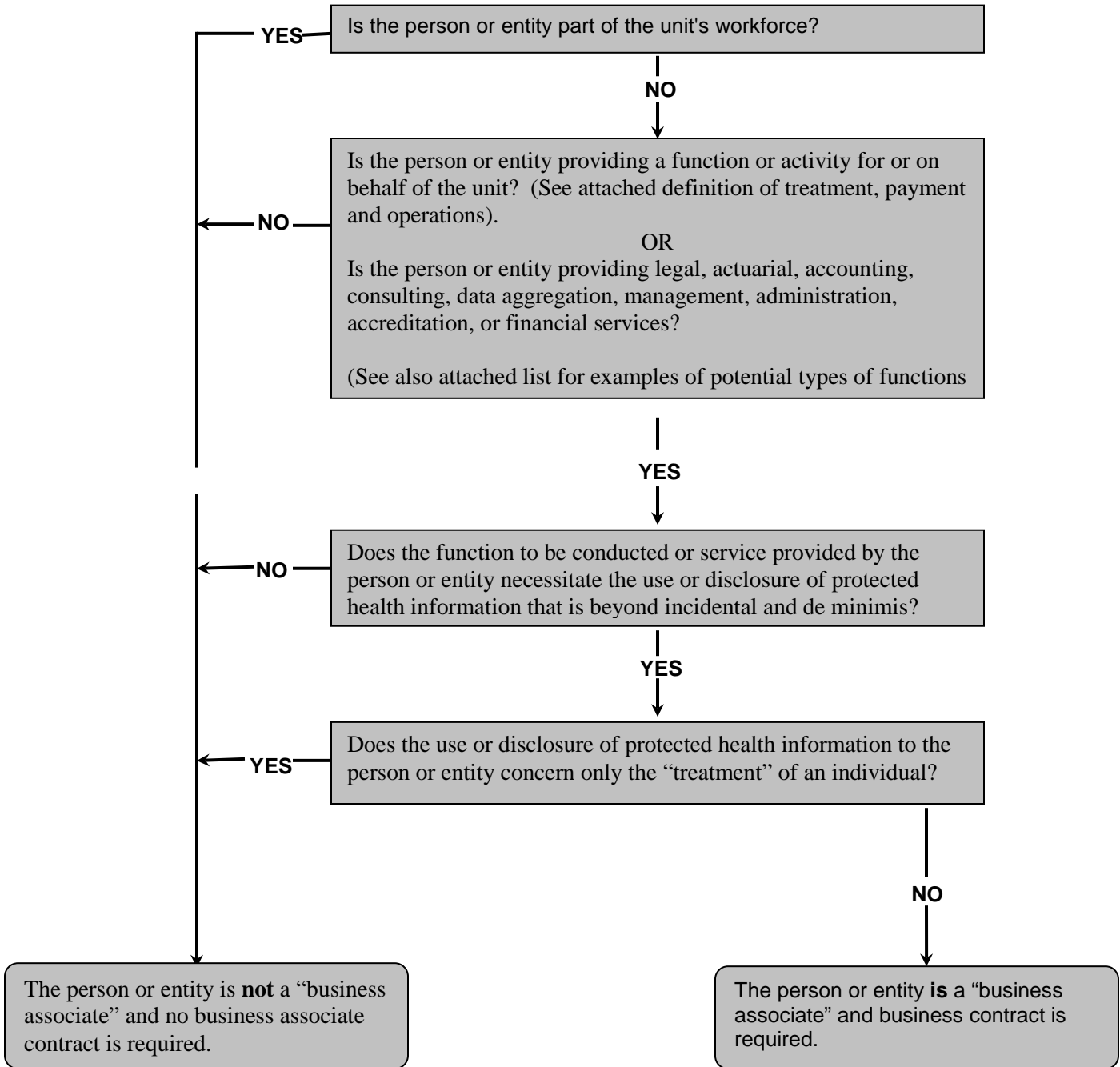


EXHIBIT B

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

This Business Associate Agreement
Is Related To and a Part of the Following
Underlying Agreement:

Effective Date of Underlying Agreement: _____

School/Unit: _____

Vendor: _____

Business Associate Agreement Involving the Access to Protected Health Information

This Business Associate Agreement (“BAA”) is entered into between The University of Medicine and Dentistry of New Jersey - [Name of School/Department/Unit] (“UMDNJ”), a body corporate and politic of the State of New Jersey having its principal administrative offices at 65 Bergen Street, Newark, New Jersey 07107 (hereinafter referred to as “Covered Entity”) and [Name and Address of Contracting Party] (hereinafter referred to as “Business Associate”) (the “Covered Entity” and “Business Associate” hereinafter collectively referred to as the “Parties”). Any conflict between the terms of this BAA and the Underlying Agreement between the Parties shall be governed by the terms of this BAA.

WHEREAS, in connection with the Underlying Agreement the Business Associate provides services to Covered Entity and Covered Entity discloses to Business Associate certain Protected Health Information that is subject to protection under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), the Health Information Technology for Economic and Clinical Health Act (Title XIII of the American Recovery and Reinvestment Act of 2009) (the “HITECH Act”), and regulations promulgated by the U.S. Department of Health and Human Services (the “HHS”) (hereinafter the “HIPAA Regulations” and the “HITECH Regulations,” respectively) and/or applicable state and/or local laws and regulations; and

WHEREAS, for good and lawful consideration and with acknowledgment of the mutual promises, set forth in the Underlying Agreement and herein, the Parties, intending to be legally bound, hereby agree as follows:

I. Definitions¹

- A. **Breach** means the unauthorized acquisition, access, use, or disclosure of protected health information (“PHI”) which compromises the security or privacy of such information in violation of HIPAA, the HITECH Act, the HIPAA Regulations, and/or the HITECH Regulations, except where a good faith belief exists that unauthorized persons to whom such information is disclosed would not reasonably have been able to retain such information. The term “**Breach**” does not include:
1. Any unintentional acquisition, access, or use of PHI by an employee or person acting under the authority of a Covered Entity or Business Associate if:
 - a. Such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or person, respectively, with the Covered Entity or Business Associate; and
 - b. Does not result in further unauthorized use or disclosure; or
 2. Any inadvertent disclosure by a person who is otherwise authorized to access PHI at a Covered Entity or Business Associate to another, similarly authorized person at the same Covered Entity, Business Associate or organized health care arrangement in which the Covered Entity participate and such information received as a result of such disclosure is not further used or disclosed in an impermissible manner.

¹ An expanded definition of the following terms as well as the definition of other relevant terms are available on UMDNJ’s website at <http://www.umdnj.edu/purchweb/vendors/index.htm> . Terms used in this Business Associate Agreement but not otherwise defined shall have the meaning ascribed to those terms in HIPAA, the HITECH Act, and any current and future regulations promulgated under HIPAA and/or the HITECH Act. See 45 C.F.R. 160.103, 164.402 and 164.501.

EXHIBIT D (continued)

- B. **Business Associate** means a service provider that receives PHI from, or creates or maintains PHI on behalf of, a Covered Entity including, but not limited to, claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefits management, practice management, re-pricing, transcription, legal, actuarial, accounting, consulting, data aggregation, administrative, accreditation or financial services, and vendors that offer personal health records to patients as part of a Covered Entity's electronic health record, where the service or function involves the use or disclosure of individually identifiable health information from the Covered Entity or from another Business Associate of the Covered Entity. A Business Associate excludes, among others, employees of Covered Entities.
- C. **Covered Entities** include (i) health care providers that transmit patient health information electronically in connection with a covered transaction, (ii) health plans (including employer-sponsored employee welfare benefit plans and self-insured employer-offered health plans), and (iii) health care clearinghouses.
- D. **Data Aggregation** means, with respect to PHI created or received by a Business Associate, the combining of PHI received by a Business Associate in its capacity as a Business Associate for more than one Covered Entity to permit data analyses that relate to the health care operations of the respective Covered Entities.
- E. **Designated Record Set** means any grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a Covered Entity that is (i) medical records and billing records about individuals, and/or (ii) enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan, used, in whole or in part, by or for the Covered Entity, to make decisions about individuals.
- F. **Electronic Protected Health Information ("Electronic PHI")** means PHI that is transmitted by or maintained in electronic media.
- G. **Individual** means the person who is the subject of PHI and includes a person who qualifies as a personal representative (45 C.F.R. 164.502(g)).
- H. **Protected Health Information ("PHI")** means physical and/or mental health and demographic information collected from an individual and created or received by a Covered Entity and/or Business Associate that identifies or could reasonably identify an individual (*i.e.*, is "individually identifiable") and is held or transmitted in any form including electronic media. PHI excludes educational records and employment records held by a Covered Entity as an employer (45 C.F.R. 164.501).
- I. **Required By Law** means that Covered Entities may use and disclose PHI without individual authorization as required by law (including by statute, regulation, or court orders) in accordance with the requirements in 45 C.F.R. 164.512(c), (e) or (f).
- J. **Unsecured PHI** means PHI not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary of HHS.

II. Permitted Uses and Disclosures of PHI by Business Associate

- A. Except as otherwise limited in this BAA, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Underlying Agreement, provided that such uses and/or further disclosures (i) do not violate the requirements of HIPAA's Business Associate contract standard at 45 C.F.R. 164.504(e)(1) and/or the HITECH Act, if done by the Covered Entity, (ii) are the minimum necessary PHI to accomplish the intended purpose, or (iii) are Required By Law.
- B. Except as otherwise limited in this BAA, Business Associate may use or disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of Business Associate, provided, however, that any such uses or disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that (i) the PHI will remain confidential and used or further disclosed only as Required By

EXHIBIT D (continued)

- Law or for the purpose for which it was disclosed to the person, and (ii) the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been Breached.
- C. Except as otherwise limited in this BAA, Business Associate may use PHI to provide Data Aggregation services to Covered Entity (42 C.F.R. 164.504(e)(2)(i)(B)).
 - D. Business Associate may use PHI to report violations of law to appropriate federal and state authorities as permitted under HIPAA and/or other federal and state laws. (45 C.F.R. 164.502(j)(1)).

III. Duties and Obligations of Business Associate Related to PHI

- A. Business Associate shall not use or disclose PHI other than as permitted or required by the Underlying Agreement, this BAA, and/or as Required By Law. Business Associate shall immediately notify Covered Entity of any use or disclosure of PHI in violation of this BAA.
- B. Business Associate shall use and implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of PHI and/or Electronic PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity.
- C. Business Associate shall notify, in writing, the Covered Entity when the Business Associate discovers a Breach of Unsecured PHI. A Breach is deemed to have been discovered by a Business Associate as of the first day on which Business Associate (by its employee, officer, or other agent) knows or would have known of such Breach by exercising reasonable diligence. Business Associate's notification to Covered Entity (i.e., UMDNJ) shall:
 - 1. Be made to the Covered Entity without unreasonable delay and in no event later than ten (10) days following the discovery of a breach, except in the case of a Business Associate that is an agent of the Covered Entity, in which case the Business Associate must provide the Covered Entity with immediate notification of the breach, except where law enforcement officials determine that a notification would impede a criminal investigation or cause damage to national security. Unless the language in the underlying agreement between the parties indicates that a Business Associate is an independent contractor, then the Business Associate shall be considered an agent of UMDNJ for purposes of breach notification.
 - 2. To the extent possible, provide the identity of each Individual whose Unsecured PHI was, or is reasonably believed to have been, Breached, and any other information that the Covered Entity is required to include in the notice to affected Individuals under 45 C.F.R. 164.404(c), either at the time of notice of Breach to the Covered Entity or as promptly thereafter as information becomes available. Include information in substantially the same form as the "Notification To the Covered Entity About A Breach of Unsecured Protected Health Information" available to Business Associates at UMDNJ's website at http://www.umdnj.edu/hipaaweb/BN/NOTIFICATION_TO_THE_COVERED_ENTITY.pdf.
- D. Business Associate is subject to the same legal requirements to cure, terminate or report violations to the Secretary of HHS under the same duty and in the same manner as Covered Entity.
- E. Business Associate shall mitigate, to the extent practicable, any harmful effect known to it resulting from an unauthorized use or disclosure of PHI or Breach of Unsecured PHI.
- F. Business Associate shall ensure that any agent, including a subcontractor, to whom it provides PHI (i) received from, or (ii) created or received by Business Associate on behalf of, a Covered Entity agrees, in writing, to the same restrictions and conditions that apply through this BAA to Business Associate with respect to such PHI.
- G. Business Associate (i) shall provide Covered Entity access to its premises for a review and demonstration of its internal practices and procedures for safeguarding PHI and, (ii) to the extent applicable, shall provide access for inspection and copying of PHI in a Designated Record Set at

EXHIBIT D (continued)

- reasonable times at the request of Covered Entity or, as directed by Covered Entity, to an Individual (45 C.F.R. 164.524). If Business Associate maintains an Electronic Health Record, Business Associate shall provide such information in electronic format to enable Covered Entity to fulfill its obligations under the HITECH Act. (42 U.S.C. §17935(e)).
- H. Business Associate shall, upon request with reasonable notice, provide Covered Entity with an accounting of uses and disclosures of PHI provided to it by Covered Entity.
 - I. Business Associate agrees to use, disclose and request (i) only the minimum necessary PHI, as defined by law, and (ii) to the extent practicable, only the limited data set of PHI excluding direct identifiers, as defined in 45 C.F.R. 164.514(e)(2).
 - J. Business Associate shall document such disclosures of PHI and information related to such disclosures as would be required for a Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI (45 C.F.R. 164.528). Should a Covered Entity or an Individual request an accounting of disclosures of PHI pursuant to 45 C.F.R. 164.528, Business Associate agrees to promptly provide Covered Entity with information in a format and manner sufficient to respond no later than sixty (60) days after receipt of such request, subject to specific statutory exceptions.
 - K. Business Associate shall make its internal practices, books and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity, available to Covered Entity at the request of Covered Entity, or the Secretary of HHS, for purposes of the Secretary determining Covered Entity's compliance with HIPAA and/or the HITECH Act in the time, manner and place designated by the Covered Entity and/or the Secretary.
 - L. To the extent applicable, Business Associate shall make any amendment(s) to PHI in a Designated Record Set that Covered Entity directs or agrees to, no later than sixty (60) days after receipt of such request from a Covered Entity or Individual.
 - M. Business Associate agrees to abide by the limitations on marketing communications to Individuals regarding the purchase and use of products or services set forth in the HITECH Act and the HITECH Regulations.
 - N. Business Associate agrees and acknowledges that the administrative rules governing, and the civil and criminal penalties for violating, HIPAA, the HITECH Act, the HIPAA Regulations and the HITECH Regulations, apply to it in the same manner as they apply to Covered Entity, as more fully set forth at UMDNJ's website at <http://www.umdnj.edu/complweb/policies/index.htm>.

IV. **Term and Termination**

- A. **Term.** The term of this BAA shall be effective as of the effective date of the Underlying Agreement and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions of this Section IV.
- B. **Termination for Cause.** Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:
 - 1. Provide an opportunity for Business Associate to cure the breach or end the violation, and terminate this BAA and the Underlying Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;
 - 2. Immediately terminate this BAA and/or the Underlying Agreement if Business Associate has breached a material term of this BAA and cure is not possible; or
 - 3. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary of HHS.

EXHIBIT D (continued)

C. Effect of Termination.

1. (a) Except as provided in paragraph C.2 of this Section, upon termination of this BAA, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of PHI.

(b) Except as provided in paragraph C.2 of this Section, if Covered Entity, in its sole discretion, requires that Business Associate destroy any or all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, either due to the termination of this BAA or otherwise, Business Associate shall certify, in writing, to Covered Entity that the PHI has been destroyed and rendered indecipherable, pursuant to HIPAA and the HITECH Act. This provision also shall apply to PHI that is in the possession of subcontractors or agents of Business Associate.
2. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity written notification of the conditions that make return or destruction infeasible within thirty (30) calendar days of such request. In such case, Business Associate shall extend the protections of this BAA to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI. This provision also shall apply to PHI that is in the possession of subcontractors or agents of Business Associate.
3. Should the Business Associate make a disclosure of PHI in violation of this BAA, Covered Entity shall have the right to immediately terminate any contract, other than this BAA, then in force between the Parties, including the Underlying Agreement.
4. The provisions of this Section IV.C. shall survive the termination of this BAA and the Underlying Agreement for any reason.

V. Remedies In Event of Breach

- A. Business Associate agrees and acknowledges that irreparable harm will result to Covered Entity, and to its business, in the event of breach by Business Associate of any covenants, duties, obligations and assurances in this BAA and further agrees that remedy at law for any such breach shall be inadequate and that damages resulting there from are not susceptible to being measured in monetary terms. In the event of any such breach or threatened breach by Business Associate, Covered Entity shall be entitled to (i) immediately enjoin and restrain Business Associate from any continuing violations and (ii) reimbursement for reasonable attorneys' fees, costs and expenses incurred as a proximate result of the breach. The remedies in this Section V shall be in addition to any action for damages and/or other remedy available to Covered Entity for such breach.
- B. Business Associate shall indemnify and hold Covered Entity, its directors, officers, employees and agents harmless from any and all liabilities, damages, reasonable attorneys' fees, costs and expenses incurred by Covered Entity as a result of a breach of this BAA caused by Business Associate's actions or inactions and/or those of its employees and agents.
- C. Business Associate agrees and acknowledges that the provisions of this BAA shall be strictly construed.

VI. Miscellaneous

- A. Independent Contractor. None of the provisions of this BAA and/or the Underlying Agreement are intended to create nor shall be deemed or construed to have created any relationship between the Parties other than that of independent entities contracting with each other unless otherwise explicitly stated in this BAA or the Underlying Agreement.

EXHIBIT D (continued)

- B. Detrimental Reliance By Covered Entity. Business Associate agrees and acknowledges that its covenants, duties, obligations and assurances herein shall be detrimentally relied upon by Covered Entity in choosing to commence or continue a business relationship with Business Associate. Covered Entity shall not be liable to Business Associate for any claim, loss, or damage relating to Business Associate's use or disclosure of any information received from Covered Entity or from any other source.
- C. Regulatory References. Any reference herein to law means the law as in effect or as amended.
- D. Construction. The BAA shall be construed broadly and any ambiguity shall be resolved in favor of a meaning that complies and is consistent with applicable law.
- E. Severability. In the event that any provision of this BAA violates any applicable statute, ordinance or rule of law in any jurisdiction that governs this BAA, such provision shall be ineffective to the extent of such violation without invalidating any other provision of this BAA.
- F. Authority. The signatories below have the right and authority to execute this BAA for their respective entities and no further approvals are necessary to create a binding agreement.
- H. Covered Entity's Notices To Business Associate. Covered Entity's Notices to Business Associate are available on UMDNJ's website at http://www.umdj.edu/hipaaweb/privacy/privacy_NPPUMDNJ03.htm. Such Notices include, but are not limited to, (i) any limitations in the Covered Entity's Notices of Privacy Practices that may affect the Business Associate, (ii) any changes in, or revocation of, permission by an Individual to use or disclose PHI, or (iii) any restriction in the use or disclosure of PHI that Covered Entity has agreed to.
- I. Compliance With State Law. Business Associate agrees and acknowledges that as the holder of individually identifiable health information it is subject to New Jersey law. In the event of any conflict between federal health care laws and New Jersey law, the Business Associate shall comply with the more restrictive provision.
- J. Conflict Among Contracts. Should there be conflict between the terms of this BAA and any other contract between the Parties (either previous or subsequent to the date of this BAA), the terms of this BAA shall control unless the Parties, in a subsequent writing, specifically otherwise provide.
- K. Modification. This BAA may only be modified by a writing signed by the Parties. The Parties agree to take such action subsequent to this BAA as necessary to amend the BAA from time to time as necessary for the Parties to comply with the requirements of any applicable law.
- K. Notices to Parties. Any notice required under this BAA to be given shall be made in writing to:

To The Covered Entity:

School/Unit/Department:

Address:

Telephone:

E-Mail:

To The Business Associate:

Name/Title: _____

Address:

Telephone:

E-Mail:

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

**By: UNIVERSITY OF MEDICINE
AND DENTISTRY OF NEW JERSEY
[COVERED ENTITY]**

By: [BUSINESS ASSOCIATE]

Approved:
Title:

Approved:
Title:

Date:
Version 1
2009-2010

Date: