UNIVERSITY PHYSICIANS OF BROOKLYN, INC.

POLICY AND PROCEDURE

		No:	
Subject:	BUSINESS ASSOCIATE AGREEMENTS	**Page** 1 **of** 4	
Prepared by:	Shoshana Milstein	**Original Issue Date:**	**NEW**
Reviewed by:	HIPAA Policy & Procedure Team	**Supersedes Date:**	**NONE**
	Renee Poncet	**Approval Date:**	**12/02**
Approved by:	HIPAA Oversight Committee	**Distribution:**	
		Issued by:	

I. **Purpose:** To ensure that all business associates (BA) enter into an appropriate contract with UPB that will provide satisfactory assurance to UPB that the business associate will appropriately safeguard the protected health information (PHI), in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its accompanying regulations.

II. **Definitions:**

Business Associate- A person who is not a member of UPB's workforce who:
1. On behalf of SUNY, performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information (IIHI), including claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management and repricing; or
2. Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to UPB, where the provision of the service involved the disclosure of IIHI from UPB.

III. Policy

A. Business Associate Agreement Content- The contract between UPB and a BA must:

1. Establish the permitted and required uses and disclosures of the information. The contract may not authorize further use or disclosure in a manner that would violate the HIPAA standards, except that:
   a. The contract may permit the BA to use or disclose PHI for the proper management and administration of the BA; and
   b. The contract may permit the BA to provide data aggregation services relating to UPB's health care operations.
2. Provide that the BA will:
   a. Not use or further disclose the information other than as stated in the contract or as required by law;
   b. Use appropriate safeguards to prevent use and disclosure of information other than as provided in the contract;
   c. Report to UPB any use or disclosure of information not provided for by the contract of which it becomes aware;
   d. Ensure that any agents and subcontractors to whom it provided PHI received from, or created by the BA on behalf of, UPB agrees to the same restrictions and conditions provided in the contract;
   e. Make available and provide access of PHI to a patient, when requested;
   f. Make available PHI for amendment and incorporate any amendments to PHI, as necessary;
   g. Make available the information required to provide an accounting of disclosures;
   h. Make its internal practices, books and records relating to the use and disclosure of PHI received from, or created on behalf of, UPB available to the Secretary of the Department of Health and Human Services (HHS) for purposes of determining UPB's compliance with the HIPAA Privacy standards; and
   i. If feasible, at termination of the contract, return or destroy all PHI received from, or created on behalf of, UPB that the BA still maintains in any form. The BA must not retain any copies of the information.
      i. If not feasible, the BA must 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.
3. Authorize UPB's termination of the contract if UPB determines that the BA has violated a material term of the contract.
   a. If termination is not feasible, UPB is required to notify the Secretary of the Department of Health and Human Services (HHS) of the un-cured breach.

B. Permitted Uses & Disclosures

1. The contract may permit the BA to **use** the information, if necessary:
   a. For the proper management and administration of the BA; or
   b. To carry out the legal responsibilities of the BA.
2. The contract may permit the BA to **disclose** the information for the above purposes, if:
   a. The disclosure is required by law; or
   b. The BA obtains reasonable assurances from the recipient that:
      i. The information will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the recipient;

ii. S/he will notify the BA of any breaches of confidentiality of which s/he becomes aware.

C. Treatment Relationships- A BA agreement is not needed for disclosures by UPB to a healthcare provider concerning the treatment of a patient.

D. Compliance- In order to ensure compliance, UPB will:

1. Investigate received complaints and other information containing substantial and credible evidence of violation(s) by a BA.
2. Take reasonable steps to cure the breach or violation of which it becomes aware. If such steps are unsuccessful, UPB will:
   a. Terminate the contract; or
   b. Report the problem to the Secretary of HHS, if termination is not feasible.

E. UPB as the BA- If UPB is a BA of another covered entity, it must comply with all the terms stated in the contract.

F. Documentation- All BA contracts must be documented and retained, as appropriate.

1. All new contracts after April 14, 2003 must have an appropriate business associate agreement.
2. All existing contracts that have been modified or renewed after October 15, 2002 must have an appropriate business associate agreement by April 14, 2003.
3. All existing contracts that have not been modified or renewed after October 15, 2002 must have an appropriate business associate agreement by April 14, 2004. However, the BA is still required to limit the use of protected health information to that which is permissible under HIPAA and make the protected health information available to UPB and the Department of Health and Human Services (HHS) upon request.

IV. Procedure

The development of the procedure section is the responsibility of the respective department. It is dependent upon the unique needs of each department's operating structure and shall be advanced and customized accordingly.

V. Responsibilities: It is the responsibility of all medical staff members and practice staff members to comply with this policy. Medical staff members include physicians as well as allied health professionals. Practice staff members include all employees, medical or other students, trainees, residents, interns, volunteers, consultants, contractors and subcontractors at the practice.

VI. Reasons for Revision- Regulatory changes

VII. Attachments- Business Associate Agreements: SUNY as Business Associate, SUNY as Covered Entity

VIII. References- Standards for Privacy of Individually Identifiable Health Information, 45 CFR §164.502(e), §164.504(e)

UNIVERSITY PHYSICIANS OF BROOKLYN

HIPAA BUSINESS ASSOCIATE AGREEMENT

CONTRACT NO(S):_____

THIS AGREEMENT is made by and between **UNIVERSITY PHYSICIANS OF BROOKLYN, INC., located at 450 Clarkson Ave., Brooklyn, NY 11203** ("Covered Entity") and _____ ("Business Associate").

Name/Address of Business Associate

Covered Entity and Business Associate, collectively, may hereinafter be referred to as the "Parties," as in the parties to this Agreement.

WHEREAS, Covered Entity and Business Associate are parties to one or more agreements and/or may in the future become parties to additional agreements (collectively, the "Underlying Agreements"), pursuant to which Business Associate provides certain services to Covered Entity and, in connection with such services, creates, receives, uses or discloses for or on behalf of Covered Entity certain individually identifiable Protected Health Information relating to patients of Covered Entity ("PHI") that is subject to protection under the Health Insurance Portability and Accountability Act of 1996 as amended by the Health Information Technology for Economic and Clinical Health Act Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act, 2009 (HITECH Act) and regulations promulgated there under, as such law and regulations may be amended from time to time (collectively, "HIPAA"); and

WHEREAS, Covered Entity and Business Associate wish to comply in all respects with the requirements of HIPAA, including requirements applicable to the relationship between a covered entity and its business associates;

NOW, THEREFORE, the parties agree that each of the Underlying Agreements shall hereby be amended as follows:

1. **Definitions.**

(a) "Breach"- means the acquisition, access, use, or disclosure of unsecured Protected Health Information which compromises the security or privacy of the Protected Health Information in a manner not permitted under subpart E of 45 CFR § 164.402 which compromises the security or privacy of the Protected Health Information. Such term does not include (i) any unintentional acquisition, access, use, or disclosure of such information by a workforce member or person acting under the authority of a Covered Entity or Business Associate involved if such acquisition, access, use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of 45 CFR § 164.402; (ii)Any inadvertent disclosure by a person who is authorized to access Protected Health Information at a Covered Entity or Business Associate to another person authorized to access Protected Health Information at the same Covered Entity or Business Associate, or organized health care arrangement in which the Covered Entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E 45 CFR § 164.402; (iii) a disclosure of Protected Health Information where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

(b) "Business Associate" shall have the same meaning given to such term as defined in 45 CFR § 160.103.

(c) "Covered Entity" shall have the same meaning given to such term as defined in 45 CFR § 160.103.

(d) "Designated Record Set" shall have the same meaning given to such term as defined in 45 CFR § 164.501.

(e) "Individual" shall have the same meaning given to such term as defined in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

(f) "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E respectively.

(g) "Protected Health Information" or "PHI" shall have the same meaning given to such term as defined in 45 CFR §160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

(h) "Electronic Protected Health Information " or "e-PHI" shall have the same meaning given to such term as defined in 45 CFR §160.103 limited to the information transmitted or maintained by the Business Associate in electronic form format or media.

(i) "Required By Law" shall have the same meaning given such term as defined in 45 CFR§ 164.103.

(j) "Security" or "Security Measures" encompass all of the administrative, physical, and technical safeguards in an information system specified in subpart C of 45, CFR § 164.

(k) "Security Rule" shall mean the Standards for Security of Electronic Protected Health Information as specified in subparts A and C in 45 C.F.R. Parts 160 and 164, respectively.

(l) "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

2. Obligations and Activities of Business Associate.

(a) Except as otherwise limited in this Agreement, Business Associates may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Underlying

Agreement, provided that such use or disclosure would not violate the Privacy and Security Rules, if done by Covered Entity

(b) Business Associate agrees to use appropriate safeguards, including without limitation, administrative, physical and technical safeguards, to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement and to reasonably and appropriately protect the confidentiality, integrity and availability of any electronic Protected Health Information (e-PHI) that it may receive, maintain or transmit on behalf of the Covered Entity.

(c) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

(d) Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement or any security incident of which it becomes aware, involving Protected Health Information of the Covered Entity.

(e) Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information. Business Associate shall not permit any Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity to be disclosed, transmitted or accessed by any employee, agent, consultant, contractor or subcontractor or any of their respective employees, agents, consultants, contractors or subcontractors not located with the continental Unites States of America, Alaska, Hawaii and the District of Columbia.

(f) Business Associate agrees to provide access, at the written request of Covered Entity, and in the time and manner designated by Covered Entity, to Protected Health Information in a Designated Record Set, to Covered Entity or, as

directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR §164.524.

(g) Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR §164.526 at the written request of Covered Entity or an Individual, and in the time and manner designated by Covered Entity.

(h) Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, or at the request of the Covered Entity to the Secretary, in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy and Security Rules.

(i) Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR §164.528.

(j) Business Associate agrees to provide to Covered Entity or an Individual, in time and manner designated by Covered Entity, information collected in accordance with Section (2)(i) of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR §164.528.

(k) Business Associate hereby acknowledges and agrees that Covered Entity has notified Business Associate that it is required to comply with the confidentiality, disclosure and re-disclosure requirements of 10 NYCRR Part 63 to the extent such requirements may be applicable.

(l) If in providing services to its patients, Business Associate regularly (not rarely or sporadically) extends, renews or continues credit to patients or regularly allows its patients to defer payment for services including setting up payment plans in

connection with one or more covered accounts (as that term is defined at 16 C.F.R. § 681.2(b)(3)), the Business Associate shall comply with the Federal Trade Commission's "Red Flag" Rules by developing and implementing a written identity theft prevention program designed to identify, detect, mitigate and respond to suspicious activities (Red Flags) that could indicate that identity theft has occurred in the Business Associate practice or business.

3. Permitted Uses and Disclosures by Business Associate.

In case Business Associate obtains or creates Protected Health Information, Business Associate may use or disclose Protected Health Information only if such use or disclosure, respectively, is in compliance with each applicable requirement of 45 CFR § 164.504(e). It means that:

(a) Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(b) Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

4. Application of Security and Privacy Provisions to Business Associate.

(a) Security Measures: 45 CFR §164.308, 164.310, 164.312 and 164.316, dealing with the administrative, physical and technical safeguards as well as policies, procedures and documentation requirements that apply to Covered Entity shall in the same manner apply to Business Associate. Any additional security requirements contained in Division A Title XIII Health Information Technology of the American Recovery and Reinvestment Act that apply to Covered Entity shall also apply to Business Associate. Pursuant to the foregoing requirements in this section, when Business Associate receives, maintains, or transmits electronic Protected Health Information (e-PHI) on behalf of the Covered Entity it will ensure the confidentiality and security as appropriate to protect such information as required by law. Business Associate will also ensure that any agent, including a subcontractor, to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect such information. Business Associates that require access to Covered Entity electronic patient systems and electronic infrastructure systems (either on site or remote) will supply the necessary information of employees to uniquely identify such employees, as employees with a need to access systems and will supply to Covered Entity Information Security Officer a valid state or federal issued photo ID for such employees to receive a unique user name and password to access the system(s).

(b) Application of Civil and Criminal Penalties- If Business Associate violates any security provision specified in subparagraph (a) above, sections 1176 and 1177 of the Social Security Act 42 U.S.C. §1320d-5, 1320d-6 shall apply to Business Associate with respect to such violation in the same manner that such sections apply to Covered Entity if it violates such security provision.

(c) Annual Guidance- For the first year beginning after the date of the enactment of the HITECH Act and annually thereafter, the Secretary shall, in consultation with industry stakeholders, annually issue guidance on the most effective and appropriate technical safeguards for use in carrying out the sections referred to in subsection (a) and the security standards in subpart C of 45 CFR § 164, as

such provisions are in effect as of the date before the enactment of this Act. Covered Entity and Business Associate shall, at their own cost and effort, monitor the issuance of such guidance and comply with them accordingly.

(d) The enhanced HIPAA privacy requirements including but not necessarily limited to accounting for certain PHI disclosures for treatment, restrictions on the sale of PHI, restrictions on marketing communications, payment and health care operations contained Subtitle D of the HITECH Act that apply to the Covered entity shall equally apply to the Business Associate.

5. Information Breach Notification Requirements.

(a) Business Associate expressly recognizes that Covered Entity has certain reporting and disclosure obligations to the Secretary of the Department of Health and Human Services and the Individual in case of a security breach of unsecured Protected Health Information. Where Business Associate accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured Protected Health Information, Business Associate without unreasonable delay and in no case later than thirty (30) days following the discovery of a breach of such information, shall notify Covered Entity of such breach. Such notice shall include the identification of each individual whose unsecured Protected Health Information has been, or is reasonably believed by the Business Associate to have been, accessed, acquired or disclosed during the breach.

(b) Covered Entity and Business Associate recognizes that the unsecured Protected Health Information may contain the social security numbers, financial account information or driver's license number or non-driver identification card number ("private information" as defined in the New York State Information Security Breach and Notification Act, as amended "ISBNA" (General Business Law § 889-aa; State Technology Law § 208). Subject to the issue of interim final regulations by the Secretary and any periodic

updates thereof all of which are incorporated by reference in this Agreement, in event of the breach of unsecured Protected Health Information containing an Individual's private information, Business Associate shall in addition to notifying Covered Entity as in subparagraph (a) comply with the provisions of the New York State Information Security Breach and Notification Act (General Business Law § 899-aa and State Technology Law, § 208). Business Associate shall be liable for the costs associated with such breach if caused by the Business Associate's negligent or willful acts or omissions, or the negligent or willful acts or omissions of Business Associate's agents, officers, employees or subcontractors

6. Term and Termination.

(a) Term. The Term of this Agreement shall be effective as of the Effective Date (as defined below), and shall terminate when all of the Protected Health Information 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 Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

(b) Termination for Cause. The parties acknowledge that in the event the Covered Entity learns of a pattern or activity or practice of the Business Associate that constitutes violation of a material term of this Agreement, then the parties promptly shall take reasonable steps to cure the violation. If such steps are, in the judgment of the Covered Entity, unsuccessful, ineffective or not feasible, then the Covered Entity may terminate, in its sole discretion, any or all of the Underlying Agreements upon written notice to the Business Associate, if feasible, and if not feasible, shall report the violation to the Secretary of the Department of Health and Human Services.

(c) Effect of Termination.

(1) Except as provided in paragraph (2) of this section, upon termination of this Agreement or the Underlying Agreement(s) for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

(2) In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

(d) Effective Date. The effective date of this Agreement (the "Effective Date") shall be the date of the last signature below.

7. Miscellaneous.

(a) Regulatory References. A reference in this Agreement to a section in the Privacy and Security Rules means the section as in effect or as amended, and for which compliance is required.

(b) Agreement. The Parties agree to take such action as is necessary to amend the Underlying Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy and Security Rules and the Health Insurance Portability and Accountability Act, Public Law §104-191; provided, however, that no Agreement shall be deemed valid unless signed by

both parties and approved by the New York State Attorney General and the Office of the State Comptroller.

(c) Survival. The respective rights and obligations of Business Associate under Section 6(c) of this Agreement shall survive the termination of this Agreement and/or the Underlying Agreements, as shall the rights of access and inspection of Covered Entity.

(d) Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with the Privacy and Security Rules.

8. Governing Law; Conflict.

This Agreement shall be enforced and construed in accordance with the laws of the State of New York. Jurisdiction of any litigation with respect to this Agreement shall be in New York, with venue in a court of competent jurisdiction located in Kings County. In the event of a conflict between the terms of this Agreement and the terms of any of the Underlying Agreements, the terms of this Agreement shall control.

University Physicians of Brooklyn - Signature of Authorized Official	Business Associate- Signature of Authorized Official
University Physicians of Brooklyn - Print Name of Authorized Official	Business Associate- Print Name of Authorized Official
Date	Date