

SUNY DOWNSTATE MEDICAL CENTER
UNIVERSITY HOSPITAL OF BROOKLYN
POLICY AND PROCEDURE

No. HIPAA-3

Subject: BUSINESS ASSOCIATE
AGREEMENTS

Page 1 of 4

Prepared by: Shoshana Milstein

Original Issue Date 12/02

Reviewed by: Maureen Crystal
Marty Deane
Brian Gaon

Supersedes: 07/06

Effective Date: 12/07

Approved by: Kevin O'Mara
Fred Hammond
Ivan fLisnitzer

The JC Standards:

Approved by: Anny Yeung, RN, MPA

Margaret Jackson, MA, RN

David Conley, MBA

Stanley Fisher, M.D.

Michael Lucchesi, M.D.

Debra D. Carey, MS

Ivan M. Lisnitzer

Issued by: Regulatory Affairs

I. **PURPOSE**

To ensure that all business associates (BA) enter into an appropriate contract with SUNY Downstate that will provide satisfactory assurance to SUNY Downstate 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. **POLICY**

A. **Business Associate Agreement Content-** The contract between SUNY Downstate 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 SUNY Downstate'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, including administrative, physical and technical safeguards, to prevent unauthorized use and disclosure other than as provided in the contract and to protect the confidentiality, integrity and availability of electronic PHI that it creates, receives, maintains or transmits on behalf of the covered entity;
 - c. Report to SUNY Downstate any use or disclosure of information not provided for by the contract or any security incident 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, SUNY Downstate 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, SUNY Downstate available to the Secretary of the Department of Health and Human Services (HHS) for purposes of determining SUNY Downstate'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, SUNY Downstate that the BA still maintains in any form. The BA must not retain any copies of the information.
 - j. 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 SUNY Downstate's termination of the contract if SUNY Downstate determines that the BA has violated a material term of the contract.
 - a. If termination is not feasible, SUNY Downstate 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 SUNY Downstate to a healthcare provider concerning the treatment of a patient.

D. Compliance- In order to ensure compliance, SUNY Downstate 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, SUNY Downstate will:
 - a. Terminate the contract; or
 - b. Report the problem to the Secretary of HHS, if termination is not feasible.

E. SUNY Downstate as the BA- If SUNY Downstate 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 SUNY Downstate and the Department of Health and Human Services (HHS) upon request.

III. DEFINITION(s)

Business Associate- A person who is not a member of SUNY Downstate'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 SUNY Downstate, where the provision of the service involved the disclosure of IIHI from SUNY Downstate.

IV. RESPONSIBILITIES

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

V. PROCEDURE/GUIDELINES

All new contracts and renewal of contracts for services that may involve PHI will incorporate BAA's, as an exhibit to and a part of such contract. Both the contractor and an authorized signatory at DMC sign all BAA's. The Contract and Procurement Department maintains all executed BAA's, as well as a database to track all vendors with a BAA.

In addition, Contracts and Procurement will, on an annual basis, review a current Vendor Disbursement Report to identify any additional vendors that may require a BAA.

If a vendor proposes revisions to the language in DMC's standard BAA, DMC's legal counsel will review such proposed revisions for acceptability.

VI. ATTACHMENTS

Business Associate Agreements: SUNY as Business Associate, SUNY as Covered Entity

VII. REFERENCES

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

	Revision	Required	Responsible Staff Name and Title
	Yes	No	Adeola O. Dabiri, Director of Regulatory Affairs
	Yes	No	
	Yes	No	

SUNY DOWNSTATE MEDICAL CENTER
HIPAA BUSINESS ASSOCIATE AGREEMENT

CONTRACT NO(S).: _____

THIS AGREEMENT is made by and between **THE STATE UNIVERSITY OF NEW YORK** ("SUNY"), an educational corporation organized and existing under the laws of the State of New York and having its principal offices located at State University Plaza, Albany, New York 12246, acting for and on behalf of **SUNY DOWNSTATE MEDICAL CENTER** (also known as SUNY Health Science Center at Brooklyn), located at 450 Clarkson Ave., Brooklyn, New York 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 with contract numbers referenced above, and 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 unauthorized acquisition, access, use, or disclosure of unsecured Protected Health Information which compromises the security, privacy, or integrity of protected health information maintained by or on behalf of a person. Such term does not include any unintentional acquisition, access, use, or disclosure of such information by an employee or agent of the Covered Entity or Business Associate involved if such acquisition, access, use, or disclosure, respectively, was made in good faith and within the course and scope of the employment or other contractual relationship of such employee or agent, respectively, with the Covered Entity or Business Associate and if such information is not further acquired, accessed, used, or disclosed by such employee or agent.

(b) “Business Associate” shall have the same meaning given to such term in § 160.103 of Title 45, Code of Federal Regulations.

(c) “Covered Entity” shall have the same meaning given to such term in § 160.103 of Title 45, Code of Federal Regulations.

(d) “Designated Record Set” shall have the same meaning as the term “designated record set” in 45 CFR 164.501.

(e) “Individual” shall have the same meaning as the term “individual” in 45 CFR 164.501 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.

(g) “Protected Health Information” shall have the same meaning as the term “protected health information” in 45 CFR 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

(h) “Required By Law” shall have the same meaning as the term “required by law” in 45 CFR 164.501.

(i) “Security” or “Security Measures” encompass all of the administrative, physical, and technical safeguards in an information system specified in § 160.103 of Title 45, Code of Federal Regulations.

(j) “Security Rule” shall mean the Standards for Security of Electronic Protected Health Information at 45 C.F.R. Parts 160 and 164, Subparts A and C.

(k) “Secretary” shall mean the Secretary of the Department of Health and Human Services or his designee.

2. Obligations and Activities of Business Associate.

(a) Business Associate agrees to not use or further disclose Protected Health Information other than as permitted or required by the Underlying Agreement or as required by law.

(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 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.

(f) Business Associate agrees to provide access, at the 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 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 § 164.504(e) Title 45, Code of Federal Regulations. It means that:

(a) Except as otherwise limited in this Agreement, Business Associate 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) 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.

(c) 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: Sections 164.308, 164.310, 164.312 and 164.316 of Title 45 of the Code of Regulations 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 Sub Title D of Title IV- Health Information Technology of the HITECH Act that apply to Covered Entity shall also apply to Business Associate. Pursuant to the foregoing requirements in this section, the Business Associate 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 or has access to and demonstrate to the Covered Entity Information Security that are in compliance with these requirements. When Business Associate receives, maintains, or transmits electronic protected health information on behalf of the covered entity they will demonstrate and ensure the confidentiality and mode of security as appropriate to protect such information to the Covered Entity Information Security Officer. 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 and each Business Associate's employee will sign Covered Entity confidentiality statement and the employee will then 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 part 164 of title 45, Code of Federal Regulations, 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, United States Congress 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 60 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 Section 899-aa and State Technology Law, Section 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. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity may, in its sole discretion, either (1) provide Business Associate with an opportunity to cure the breach and then terminate the Underlying Agreement if Business Associate does not cure the breach within time period specified by the Covered Entity or (2) terminate the Underlying Agreement immediately.

(c) Effect of Termination.

(1) Except as provided in paragraph (2) of this section, upon termination of this Agreement or the Underlying Agreement 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 later of (i) the effective date of the Underlying Agreement or (ii) April 14, 2003.

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, when applicable.

(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. Material Breach.

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.

9. 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.

SUNY Downstate Medical Center-
Signature of Authorized Official

Business Associate-
Signature of Authorized Official

SUNY Downstate Medical Center-
Print Name of Authorized Official

Business Associate-
Print Name of Authorized Official

Date

Date