

NEW YORK UNIVERSITY

HIPAA Information Security Policies, Specifications, and Definitions

Policy 10. Business Associate Contracts and Other Arrangements

Responsible Officer: Associate Provost and Chief Information Technology Officer
Effective Date: January 1, 2005
Compliance Deadline: April 21, 2005
Date of Latest Revision: December 23, 2004

POLICY STATEMENT

New York University strives to protect the *confidentiality, integrity, and availability* of *EPHI* by permitting a *business associate* to create, receive, maintain, or transmit *EPHI* on its behalf only if there is a written agreement between New York University and the *business associate* that provides assurances that the *business associate* will appropriately safeguard such *EPHI*. Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

REASON FOR POLICY

New York University must obtain satisfactory assurances from *business associates* that they will appropriately safeguard *EPHI* as required by the *HIPAA Security Regulations*. This policy reflects New York University's commitment to comply with such Regulations.

OPERATIONAL REQUIREMENTS

- A. New York University and its *covered components* must obtain assurances from a *business associate* that it will appropriately safeguard *EPHI*; such assurances must be documented in writing in a *business associate* agreement/addendum between New York University and the *business associate*. New York University's standard *business associate* agreement/addendum is attached to this policy as EXHIBIT 10A. Neither New York University nor any *covered component* may modify the attached form of *business associate* agreement/addendum, or execute any other form of *business associate* agreement (e.g., a form provided by the *business associate*), without the approval of New York University's Office of Legal Counsel.
- B. *New York University workforce* members shall not disclose any *EPHI* to a *business associate*, or permit a *business associate* to create, receive, maintain, or transmit *EPHI* on behalf of New York University, unless the *business associate* has signed a *business associate* agreement/addendum with New York University in accordance with this policy.
- C. A copy of each *business associate* agreement/addendum shall be retained in accordance with New York University's and each *covered component's* customary procedures.

D. HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards

TYPE: Standard, plus REQUIRED Implementation Specification for Business Associate Contracts Standard

HIPAA HEADING: Business Associate Contracts and Other Arrangements; Written Contract or Other Arrangement

REFERENCE: 45 CFR 164.308(b)(1); 45 CFR 164.308(b)(4)

SECURITY REGULATION STANDARDS LANGUAGE: “A covered entity, in accordance with § 164.306 [Security standard: General rules], may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity’s behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a)[Business associate contracts and other arrangements] that that the business associate will appropriately safeguard the information.”

DEFINITIONS

Availability

Business associate

Confidentiality

Covered component

Electronic Protected Health Information (or EPHI)

HIPAA Security Regulations

Integrity

Workforce member

RELATED HIPAA DOCUMENTS

HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation

HIPAA Privacy Regulations Business Associate Policy

HIPAA Privacy Regulations covered component’s Minimum Necessary Policy

Public Law 104-191, August 21, 1996, Health Insurance Portability and Accountability Act of 1996,

<<http://aspe.os.dhhs.gov/admsimp/pl104191.htm>>.

Part II, Department of Health and Human Services, 45 CFR Parts 160, 162, and 164 Health Insurance

Reform: Security Standards; Final Rule, February 20, 2003, <<http://aspe.hhs.gov/admsimp/FINAL/FR03-8334.pdf>>.

EXHIBIT 10A

BUSINESS ASSOCIATE AGREEMENT/ADDENDUM

(Privacy and Security)

This Business Associate Agreement/Addendum (“BA Agreement”) is effective as of _____, 2003 (the “Effective Date”) by and between New York University, for its _____, (“Covered Entity”) and _____ (“Business Associate”).

1. Definitions

a. “HIPAA” means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

b. “HIPAA Regulations” means the regulations promulgated under HIPAA by the United States Department of Health and Human Services, including, but not

limited to, 45 CFR Part 160 and 45 CFR Part 164, as in effect or as amended from time to time.

- c. Any capitalized terms used, but not otherwise defined, in this BA Agreement

shall have the same meaning as those terms have under HIPAA and the HIPAA Regulations.

2. **Obligations and Activities of Business Associate**

- a. *Covered Information.* Business Associate acknowledges and agrees that all

Protected Health Information ("PHI") that is created or received by Covered Entity and disclosed or made available in any form, including paper record, oral communication, audio recording, and electronic display, by Covered Entity to Business Associate or is created or received by Business Associate on Covered Entity's behalf shall be subject to this Agreement.

- b. *Use or Disclosure.* Business Associate agrees not to use or further disclose PHI created or received by Business Associate from, or on behalf of, Covered Entity ("PHI") other than as expressly permitted or required by this BA Agreement or as required by law.

- c. *Safeguards.* Business Associate agrees to use appropriate safeguards to prevent any use or disclosure of the PHI other than uses and disclosures expressly provided for by this BA Agreement. Business Associate will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic PHI that it creates, receives, maintains or transmits on behalf of Covered Entity as required by the HIPAA Regulations.

- d. *Mitigation.* Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this BA Agreement.

- e. *Reporting.* Business Associate agrees to report to Covered Entity any use or disclosure of the PHI in violation of this BA Agreement of which it becomes aware as soon as reasonably practicable. In addition, Business Associate shall report to Covered Entity any Security Incident of which it becomes aware.

- f. *Subcontractors and Agents.* Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides PHI agrees to the same restrictions and conditions, including but not limited to the implementation of reasonable and appropriate safeguards to protect Electronic PHI, that apply through this BA Agreement to Business Associate with respect to such information.

g. *Access.* If Business Associate has PHI in a Designated Record Set, Business Associate agrees to provide access, when requested by Covered Entity, to PHI in a Designated Record Set to Covered Entity or to an Individual in order to comply with the requirements under 45 CFR 164.524 and the policies of Covered Entity. Such access shall be provided by Business Associate in the time and manner designated by Covered Entity.

h. *Amendment.* If Business Associate has PHI in a Designated Record Set, when requested by Covered Entity or an Individual, Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526 and the policies of Covered Entity. Such amendments shall be made by Business Associate in the time and manner designated by Covered Entity.

i. *Audit and Inspection.* Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI available to the Covered Entity or to the Secretary of Health and Human Services or his or her designee ("Secretary") for the purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule. Such information shall be made available in the time and manner designated by the Covered Entity or the Secretary.

j. *Documentation of Disclosures.* Business Associate agrees to document such disclosures of PHI and any 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 PHI in accordance with 45 CFR 164.528 and the policies of Covered Entity.

k. *Accounting.* Business Associate agrees to provide to Covered Entity or an Individual information collected in accordance with Section 2.i. of this BA Agreement to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR 164.528 and the policies of Covered Entity. Such information shall be provided in the time and manner designated by the Covered Entity.

3. Permitted Uses and Disclosures by Business Associate

a. *Services.* Except as otherwise limited in this BA Agreement, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity in connection with [*the performance of the services listed in Exhibit A, as may be amended from time to time, annexed to this Agreement (the "Services")*] OR [*the services rendered by Business Associate pursuant to the agreement between the parties dated _____*] if such use or disclosure of PHI would not violate HIPAA or the HIPAA Regulations if done by Covered Entity or the Minimum Necessary policies and procedures of the Covered Entity.

b. *Business Activities.* Except as otherwise limited in this BA Agreement, Business Associate may use PHI for the proper management and administration of the Business Associate or to meet its legal responsibilities.

4. Obligations of Covered Entity

Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity or that is not otherwise expressly permitted under this BA Agreement.

5. Term and Termination

a. *Term.* This BA Agreement shall be effective as of the Effective Date and shall continue unless or until the BA Agreement is terminated in accordance with the provisions of Section 5.b. or 6.a.

b. *Termination.* Covered Entity may terminate this BA Agreement upon thirty days prior written notice to Business Associate or, upon written notice to Business Associate when Covered Entity determines that no further services will be provided by Business Associate or any underlying agreement between the parties relating to the services provided is terminated. In addition, 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 this BA Agreement and its relationship with Business Associate, including any underlying agreement relating to the services provided, if Business Associate does not cure the breach within the time period specified by the Covered Entity, (2) terminate this BA Agreement and the relationship between the parties, including any underlying agreement relating to the services provided, immediately, or (3) if neither termination nor cure is feasible, report the violation to the Secretary.

c. *Effect of Termination.*

(1) Upon termination of this BA Agreement, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity. This provision shall also apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.

(2) Notwithstanding the foregoing, in the event that Business Associate determines that returning or destroying the PHI 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 PHI is infeasible, Business Associate shall extend the protections of this BA Agreement 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.

6. Miscellaneous

a. *Amendment.* Covered Entity and Business Associate agree to amend this BA Agreement from time to time as may be required to ensure that Covered Entity and Business Associate comply with changes in state and federal laws and regulations relating to the privacy, security and confidentiality of PHI. Covered Entity may terminate this BA Agreement upon thirty (30) days written notice in the event that Business Associate does not promptly enter into an amendment that Covered Entity, in its sole discretion, deems sufficient to ensure that Covered Entity will be able to comply with such laws and regulations.

b. *Survival.* The respective rights and obligations of Business Associate under Section 5.c. of this BA Agreement shall survive the termination of this BA Agreement.

c. *Interpretation.* Any ambiguity in this BA Agreement shall be resolved in favor of a meaning that permits Covered Entity to comply with applicable law protecting the privacy, security and confidentiality of PHI, including but not limited to, HIPAA and the HIPAA Regulations. To the extent that any provisions of this BA Agreement conflict with the provisions of any other agreement or understanding between the parties, this BA Agreement shall control.

d. *State Law.* Nothing in this BA Agreement shall be construed to require Business Associate to use or disclose PHI without a written authorization from an individual who is a subject of the PHI, or written authorization from any other person, where such authorization would be required under state law for such use or disclosure. In addition, this Agreement shall be governed by the law of the State of New York, without regard to its conflict of laws.

e. *Injunctions.* Covered Entity and Business Associate agree that any violation of the provisions of this BA Agreement may cause irreparable harm to Covered Entity. Accordingly, in addition to any other remedies available to Covered Entity at law or in equity, Covered Entity shall be entitled to an injunction or other decree of specific performance with respect to any violation of this BA Agreement or explicit threat thereof, without any bond or other security being required and without the necessity of demonstrating actual damages.

f. *Indemnification.* Business Associate shall indemnify, hold harmless defend Covered Entity from and against any and all claims, losses, liabilities, costs and other expenses resulting from, or relating to, the acts or omissions of Business Associate in connection with the representations, duties and obligations of Business Associate under this BA Agreement.

g. *No Third Party Beneficiaries.* Nothing express or implied in this BA Agreement is intended or shall be deemed to confer upon any person other than Covered Entity, Business Associate, and their respective successors and assigns, any rights, obligations, remedies or liabilities.

IN WITNESS WHEREOF, the parties hereto have duly executed this BA Agreement as of the Effective Date.

New York University for its

—

Name:
Title:

[BUSINESS ASSOCIATE]

—

Name:
Title:

(Dev. 5-03)

EXHIBIT A

SERVICES