

BUSINESS ASSOCIATE ADDENDUM

This Business Associate Addendum (“Addendum”) is effective as of _____ (the “Effective Date”) by and between The Mount Sinai Hospital and Mount Sinai School of Medicine of New York University (individually and collectively “Covered Entity”) and _____ (“Business Associate”). This Addendum supplements and is made a part of any agreements between Covered Entity and Business Associate involving the use or disclosure of PHI (as defined below). Each individual agreement is referred to herein as the “Underlying Agreement”.

1. Definitions

a. “HIPAA” means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as amended by the security provisions of the American Recovery and Reinvestment Act of 2009 (also known as the Health Information Technology for Economic and Clinical Health Act, the “HITECH Act”).

b. “HIPAA Regulations” means the regulations promulgated under HIPAA and the HITECH Act by the United States Department of Health and Human Services (“HHS”), including, but not limited to, 45 CFR Parts 160, 162 and 164 as in effect or as amended from time to time.

c. “Security Rule” means the requirements of the HIPAA Regulations pertaining to the standards for the security of electronic Protected Health Information.

d. Any capitalized terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms have under HIPAA and the HIPAA Regulations.

2. Obligations and Activities of Business Associate

a. *Use or Disclosure.* Business Associate agrees not to use or further disclose Protected Health Information created or received by Business Associate from, or on behalf of, Covered Entity (“PHI”) other than as expressly permitted or required by this Addendum or as required by law.

b. *Safeguards.* Business Associate has implemented administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the PHI, including electronic PHI, that it creates, receives, maintains or transmits on behalf of Covered Entity. Business Associate covenants that as of the HITECH Act BA Enforcement Date (as hereinafter defined), such safeguards shall include, without limitation, implementing written policies and procedures in compliance with HIPAA and the HITECH Act, conducting a security risk assessment, and training Business Associate employees, agents and independent contractors who will have access to PHI with respect to the policies and procedures required by HIPAA and the HITECH Act. The “HITECH Act BA Enforcement Date” shall be later to occur of: (i) the Effective Date of this Agreement, (ii) February 17, 2010, and (iii) the

date on which HHS will, pursuant to a written regulation, announcement or guidance, commence enforcement of the provisions of the HITECH Act that apply to Business Associates.

Business Associate shall provide Covered Entity with a copy of its written information security policies and procedures upon request.

Upon reasonable notice and during normal business hours, Covered Entity shall have the right to audit Business Associate's compliance with its security program and the terms of this Agreement. Business Associate shall cooperate in such audits and shall provide copies of any documents reasonably requested by Covered Entity at no charge.

c. *Reporting of Breaches.* In the event of a Breach (as hereinafter defined) of any Unsecured (as hereinafter defined) PHI that Business Associate accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds or uses on behalf of Covered Entity, Business Associate shall report such Breach to Covered Entity immediately, but in no event more than two (2) days after discovering the Breach. "Breach" shall mean the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information. "Unsecured" shall mean PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary from time to time.

Notice of a Breach shall include all information known to the Business Associate within two (2) business days of discovering the Breach, including the scope of the Breach (e.g. the numbers of individuals affected and PHI elements included), the date of the Breach, the circumstances surrounding the Breach, and the Business Associate's plans to investigate and mitigate the Breach. During its investigation, the Business Associate shall provide updates on the status and findings to Covered Entity's Privacy Official. Upon the conclusion of its investigation, Business Associate shall provide a written report to Covered Entity which shall include, at a minimum: (i) the identification of each individual whose PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed during the Breach, (ii) the date of the Breach, if known, (iii) the scope of the Breach, and (iv) a description of the Business Associate's response to the Breach.

In the event of a Breach, Business Associate shall, in consultation with Covered Entity, mitigate, to the extent practical, any harmful effect of such Breach that is known to Business Associate.

d. *Reporting of Improper Disclosures.* Business Associate shall track all disclosures of PHI to third parties, including those made to Business Associate's subcontractors, affiliates, agents, and representatives, other than those disclosures that meet the exception criteria of HIPAA and the HITECH Act.

Business Associate shall report to Covered Entity any instance of unauthorized or improper use or disclosure of any PHI regarding the terms and conditions of this Addendum or applicable federal and state laws as soon as practicable, but in no event later than two (2) business days of the date on which Business Associate becomes aware of such use or disclosure. In the event of an improper use or disclosure of PHI, Business Associate shall, in consultation

with Covered Entity, mitigate, to the extent practical, any harmful effect of such improper use or disclosure that is known to Business Associate.

e. *Reporting of Security Incidents.* Business Associate shall report in writing to Covered Entity within two (2) business days of becoming aware of any Security Incident involving electronic PHI, and as reasonably appropriate, shall advise Covered Entity of measures Business Associate will be taking to mitigate harm from such Security Incident, and to prevent similar future incidents.

f. *Subcontractors and Agents.* Business Associate shall obtain and maintain an written agreement with each third party, agent, and subcontractor that has or will have access to PHI, which is received from, or created or received by, Business Associate on behalf of Covered Entity, pursuant to which agreement such third party, agent, or subcontractor agrees to be bound by the same restrictions, terms, and conditions that apply to Business Associate pursuant to this Addendum with respect to such PHI.

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 New York State law applicable to Covered Entity. Such access shall be provided by Business Associate in the time and manner reasonably designated by Covered Entity.

h. *Amendment.* If Business Associate has PHI in a Designated Record Set, when requested by Covered Entity, 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 New York State law applicable to Covered Entity. Such amendments shall be made by Business Associate in the time and manner reasonably designated by Covered Entity.

i. *Audit and Inspection.* Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of Health and Human Services or his or her designee ("Secretary") or to the Covered Entity if the Secretary requires the Covered Entity to obtain such information from the Business Associate 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 reasonably 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 the HIPAA Regulations, the HITECH Act and New York State law applicable to Covered Entity.

k. *Accounting.* Business Associate agrees to provide to Covered Entity the information collected in accordance with Section 2.j. of this Addendum to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with the HIPAA Regulations, the HITECH Act and New York State law applicable to Covered

Entity. Such information shall be provided to Covered Entity promptly after the date of such disclosures and shall include (a) the date of the disclosure; (b) the name of the entity or person who received the PHI; (c) a brief description of the PHI disclosed; and (d) a brief statement of the purpose of such disclosure that includes an explanation of the basis for such disclosure. Such information shall be submitted to the Privacy Officer, Box 1111, Mount Sinai Medical Center, One Gustave L. Levy Place, New York, New York, 10029.

1. *Requests from Individuals.* In the event that any Individual requests access to, amendment of, or accounting of PHI directly from Business Associate, Business Associate shall, within two business days of receipt, forward such request to Covered Entity's Privacy Officer at the address listed above. Covered Entity shall be responsible for responding to such forwarded requests.

3. Permitted Uses and Disclosures by Business Associate

a. *Services.* Except as otherwise limited in this Addendum, 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 if such use or disclosure of PHI would not violate HIPAA or the HIPAA Regulations if done by Covered Entity.

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

c. *Minimum Necessary.* Business Associate agrees that it shall only use and disclose the minimum amount of PHI necessary for the accomplishment of the Business Associate's purpose in making the use or disclosure.

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 HIPAA or the HIPAA Regulations if done by Covered Entity or that is not otherwise expressly permitted under this Addendum.

5. Term and Termination

a. *Term.* If the parties enter into one or more separate Underlying Agreements, this Addendum shall become effective on the effective date of each such Underlying Agreement and shall terminate, with respect to a specific Underlying Agreement, upon the termination or expiration of the Underlying Agreement and when all PHI provided by either party to the other, or created or received by Business Associate on behalf of Covered Entity is destroyed or returned to Covered Entity or, if it is not feasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the terms of this Addendum.

b. *Termination for Cause.* Where Covered Entity has knowledge of a material Breach by Business Associate, and cure is possible, Covered Entity shall provide Business Associate with an opportunity to cure. Where said Breach is not cured within ten (10) business days of Business Associate's receipt of notice from Covered Entity of said Breach (or cured within thirty (30) days following notice of the Breach if the Breach is not susceptible to cure within ten (10) business days and cure is commenced by Business Associate within ten (10) business days following notice of the Breach and diligently pursued by Business Associate), Covered Entity shall terminate the Underlying Agreement, or, at Covered Entity's option, the portion of the Underlying Agreement affected by the breach.

Where Covered Entity has knowledge of a material breach of this Addendum by Business Associate, and cure is not possible, Covered Entity shall terminate the Underlying Agreement, or, at Covered Entity's option, the portion of the Underlying Agreement affected by the breach.

Where Business Associate has knowledge of a material breach of this Addendum by Covered Entity, Business Associate shall give Covered Entity notice of such breach and an opportunity to cure. If cure is not possible, Business Associate shall terminate the portion of the Underlying Agreement affected by the breach.

Where neither cure nor termination is feasible, the non-breaching party shall report the violation to the Secretary.

c. *Effect of Termination.*

(1) Upon termination of the Underlying 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. Business Associate shall promptly provide written confirmation of such return or destruction to the Covered Entity.

(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 Addendum 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 Addendum 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 the Underlying 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 reasonable 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 and 6.f of this Addendum shall survive the termination of this Addendum.

c. *Interpretation.* Any ambiguity in this Addendum 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, the HITECH Act and the HIPAA Regulations. To the extent that any provisions of this Addendum conflict with the provisions of any other agreement or understanding between the parties, this Addendum shall control.

d. *State Law.* Nothing in this Addendum 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 an Individual's Personal Representative, where such authorization would be required under state law for such use or disclosure.

e. *Injunctions.* Covered Entity and Business Associate agree that any violation of the provisions of this Addendum 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 seek an injunction or other decree of specific performance with respect to any violation of this Addendum 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 and 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 Addendum.

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

h. *Signatures.* This Addendum may be executed in counterparts, each of which when so executed and delivered shall be deemed an original and all of which taken together shall constitute one instrument. This Addendum and any counterpart original may be executed and transmitted by facsimile. The facsimile signature shall be valid and acceptable for all purposes as if it were an original.

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

COVERED ENTITY

By: _____
Name:
Title:

BUSINESS ASSOCIATE

By: _____
Name:
Title:

MR 235 (Rev. 3-10)