BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("**Agreement**") is entered into as of_____("**Effective Date**") by and between The Trustees of Columbia University in the City of New York, a New York not-for-profit corporation ("**Covered Entity**") and_____("**Business Associate**"). Each of Covered Entity and Business Associate may be referenced in this Agreement as a "**Party**" and collectively as the "**Parties**."

The Parties, intending to be legally bound, hereby agree as follows:

I. **Definitions**.

a. Except as otherwise defined in this Agreement, all capitalized terms used in this Agreement shall have the meanings set forth in HIPAA.

b. "**Breach**" shall mean the acquisition, access, use or disclosure of Protected Health Information in a manner not permitted by the HIPAA Privacy Rule that compromises the security or privacy of the Protected Health Information as defined, and subject to the exceptions set forth, in 45 CFR § 164.402.

c. "**Electronic Protected Health Information**" shall mean Protected Health Information that is transmitted or maintained in Electronic Media.

d. "**HIPAA**" shall mean the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, as amended, and supplemented by the HITECH Act and its implementing regulations, as each is amended from time to time.

e. "**HIPAA Breach Notification Rule**" shall mean the federal breach notification regulations, as amended from time to time, issued under HIPAA and set forth in 45 C.F.R. Part 164 (Subpart D).

f. "**HIPAA Privacy Rule**" shall mean the federal privacy regulations, as amended from time to time, issued under HIPAA and set forth in 45 C.F.R. Parts 160 and 164 (Subparts A & E).

g. "**HIPAA Security Rule**" shall mean the federal security regulations, as amended from time to time, issued under HIPAA and set forth in 45 C.F.R. Parts 160 and 164 (Subparts A & C).

h. "**HITECH Act**" shall mean Subtitle D of the Health Information Technology for Economic and Clinical Health Act provisions of the American Recovery and Reinvestment Act of 2009, 42 U.S.C. §§ 17921-17954, and all its implementing regulations, when and as each is effective, and compliance is required.

i. "**Protected Health Information or PHI**" shall mean Protected Health Information, as defined in 45 CFR § 160.103, and is limited to the Protected Health Information received, maintained, created, or transmitted on behalf of, Covered Entity by Business Associate in performance of the Underlying Services.

j. "**Underlying Services**" shall mean, to the extent and only to the extent they involve the creation, maintenance, use, disclosure or transmission of Protected Health Information, the services performed by Business Associate for Covered Entity pursuant to the Underlying Services Agreement.

k. "**Underlying Services Agreement**" shall mean the written agreement(s) (other than this Agreement) by and between the parties as amended as set forth in the attached schedule by and between the Parties pursuant to which Business Associate access to, receives, maintains, creates or transmits PHI for or on behalf of Covered Entity in connection with the provision of the services described in that agreement(s) by Business Associate to Covered Entity or in performance of Business Associate's obligations under such agreement(s).

II. **Permitted and Required Uses and Disclosures of Protected Health Information by Business Associate.**

a. Business Associate may use or disclose Protected Health Information solely (1) as necessary to provide the Underlying Services to Covered Entity and in compliance with each applicable requirement of 45 CFR §164.504(e),

(2) as Required by Law or (3) as expressly otherwise authorized under this Agreement. Business Associate shall not use or disclose Protected Health Information for any other purpose or in any other manner.

(1) Business Associate may, if necessary, use or disclose Protected Health Information for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate; provided, that (1) any disclosure is Required by Law or (2) Business Associate obtains reasonable advance written assurances from the person or party to whom the Protected Health Information is disclosed that (Y) the Protected Health 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 person or party, and (Z) the person or party immediately notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

III. **Obligations of Business Associate**.

a. Business Associate shall use appropriate safeguards, and comply, where applicable, with the HIPAA Security Rule with respect to Electronic Protected Health Information, to prevent use or disclosure of the information other than as provided for by this Agreement. Business Associate shall maintain an appropriate level of security with regard to all personnel, systems, and administrative processes used by Business Associate to transmit, store, process, or otherwise handle PHI. Business Associate shall not transmit PHI over any open network unless the transmission is encrypted or otherwise secured according to the appropriate standard of care. Accordingly, Business Associate shall (i) comply with the Security Rule; (ii) implement Administrative Safeguards, Physical Safeguards, and Technical Safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic PHI that it creates, receives, maintains, or transmits on behalf of Columbia as required by section 164.314(a) of the Security Rule and in accordance with the National Institute of Standards and Technology ("NIST") Cybersecurity Framework

b. Business Associate shall mitigate any harmful effect of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

c. Business Associate shall immediately report to Covered Entity: (i) any use or disclosure of Protected Health Information not provided for by this Agreement of which it becomes aware in accordance with 45 CFR § 164.504(e)(2)(ii)(C); and/or (ii) any Security Incident of which Business Associate becomes aware in accordance with 45 CFR § 164.314(a)(2)(i)(C).

d. Business Associate shall notify the Covered Entity within ten (10) days after Business Associate's Discovery of any incident that involves an unauthorized acquisition, access, use, or disclosure of Protected Health Information, even if Business Associate believes the incident will not rise to the level of a Breach. Business Associate agrees that such notification will meet the requirements of the HIPAA Breach Notification Rule set forth in 45 CFR § 164.410. Business Associate shall provide to the Covered Entity the names and contact information of all individuals whose Protected Health Information was or is believed to have been involved, all other information reasonably requested by the Covered Entity to enable the Covered Entity to perform and document a risk assessment in accordance with the HIPAA Breach Notification Rule with respect to the incident to determine whether a Breach occurred, and all other information reasonably necessary to provide notice to Individuals, the Department of Health and Human Services and/or the media in accordance with the HIPAA Breach Notification Rule. In the event of an incident that is required to be reported under this Section III(d), Covered Entity shall elect in its sole discretion whether Covered Entity, Business Associate or a third party shall be responsible for conducting an investigation of that incident and providing any required notices as set forth in this Section III(d). In accordance with this election, and notwithstanding anything to the contrary in this Agreement and without limiting in any way any other remedy available to Covered Entity at law, equity or contract, including but not limited to under Section V(a) of this Agreement, Business Associate shall (i) conduct, or pay the costs of conducting, an investigation of any incident required to be reported under this Section III(d), (ii) shall reimburse and pay Covered Entity for all expenses and costs incurred by Covered Entity that arise from an investigation of any incident required to be reported under this Section III(d) and (iii) shall provide, and/or pay the costs of providing, the required notices as set forth in this Section III(d).

e. In accordance with 45 CFR 164.502(e)(1)(ii) and 45 CFR 164.308(b)(2), Business Associate shall ensure that any subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of Business Associate, agree to the same restrictions and conditions, in writing, that apply through this Agreement

to Business Associate with respect to such Protected Health Information, including but not limited to the extent that subcontractors create, receive, maintain, or transmit Electronic Protected Health Information on behalf of the Business Associate, it shall require the subcontractors to comply with the HIPAA Security Rule.

f. To the extent Business Associate is to carry out Covered Entity's obligations under the HIPAA Privacy Rule, Business Associate shall comply with the requirements of the HIPAA Privacy Rule that apply to Covered Entity in the performance of such obligations.

g. Business Associate shall provide access to Covered Entity, no later than fifteen (15) days after receipt of a request from Covered Entity, to Protected Health Information in a Designated Record Set, or, if requested by Covered Entity, to an Individual, all in accordance with the requirements under 45 CFR § 164.524, including providing or sending a copy to a designated third party and providing or sending a copy in electronic format, to the extent that the Protected Health Information in Business Associate's possession constitutes a Designated Record Set.

h. Business Associate shall make available and make any amendment(s) to Protected Health Information in a Designated Record Set within fifteen (15) days after receipt of a request from Covered Entity or an Individual, all in accordance with the requirements of 45 CFR § 164.526.

i. Business Associate shall document 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 and, as of the date compliance is required by final regulations, 42 U.S.C. § 17935(c).

j. Business Associate shall make available to Covered Entity, within fifteen (15) days after receipt of a request, information collected in accordance with Section III(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, or make that information available directly to an Individual, all in accordance with 45 CFR § 164.528 and, as of the date compliance is required by final regulations, 42 U.S.C. § 17935(c).

k. Business Associate shall notify Covered Entity in writing within three (3) days after Business Associate's receipt directly from an Individual of any request for access to or amendment of Protected Health Information, or an accounting of disclosures, as contemplated in Sections III(g), III(h), III(i) and III(j) of this Agreement.

l. Business Associate agrees to make its internal practices, books, and records, including policies and procedures and Protected Health Information, 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 to the Secretary, for purposes of the Secretary determining Covered Entity's compliance with HIPAA.

m. Business Associate shall request, use and/or disclose only the minimum amount of Protected Health Information necessary to accomplish the purpose of the request, use or disclosure; and comply with 45 CFR §§ 164.502(b) and 164.514(d).

n. Business Associate shall not directly or indirectly receive remuneration in exchange for any Protected Health Information as prohibited by 45 CFR § 164.502(a)(5)(ii).

o. Business Associate shall not make or cause to be made any communication about a product or service that is prohibited by 45 CFR §§ 164.501 and 164.508(a)(3).

p. Business Associate shall not make or cause to be made any written fundraising communication that is prohibited by 45 CFR § 164.514(f).

q. Business Associate shall take all necessary steps, at the request of Covered Entity, to comply with requests by Individuals not to send Protected Health Information to a Health Plan in accordance with 45 CFR § 164.522(a).

r. Business Associate shall take reasonable steps to ensure that its employees' actions or omissions do not cause Business Associate to breach the terms of this Agreement or violate provisions of HIPAA that apply to Business Associate.

IV. **Term and Termination**.

a. The term of this Agreement shall commence as of the Effective Date and shall terminate concurrently with the Underlying Services Agreement unless earlier terminated, by mutual written agreement of the Parties, or in accordance with this Section IV.

b. Notwithstanding anything in this Agreement to the contrary, if Covered Entity knows of a pattern of activity or practice of Business Associate that constitutes a material breach or violation of this Agreement then Covered Entity shall provide written notice of the breach or violation to Business Associate that specifies the nature of the breach or violation. Business Associate must cure the breach or end the violation on or before thirty (30) days after receipt of the written notice. In the absence of a cure reasonably satisfactory to Covered Entity within the specified timeframe, or in the event the breach is reasonably incapable of cure, then Covered Entity may, terminate this Agreement.

c. Within thirty (30) days after termination or expiration of this Agreement, Business Associate will return or destroy, if feasible, all Protected Health Information received from or created or received by Business Associate, including all Protected Health Information in possession of Business Associate's agents or subcontractors, on behalf of Covered Entity that Business Associate still maintains in any form and retain no copies of such information. To the extent return or destruction of the Protected Health Information is not feasible, Business Associate shall notify Covered Entity in writing of the reasons return or destruction is not feasible and, if Covered Entity agrees, may retain the Protected Health Information subject to this Section. Under any circumstances, Business Associate shall extend any and all protections, limitations and restrictions contained in this Agreement to Business Associate's use and/or disclosure of any Protected Health Information retained after the expiration or termination of this Agreement and shall limit further uses and disclosures to those purposes that make the return or destruction of the information not feasible.

V. Miscellaneous.

a. Business Associate shall defend, hold harmless and indemnify Covered Entity, its trustees, officers, faculty, employees, students, against all expenses, liabilities, damages, claims, costs, fines, penalties and losses (including attorneys' and consultant fees) (collectively, "Losses") reasonably incurred by Covered Entity in connection with, related to or arising from (i) the negligent or fraudulent act or omission of Business Associate, its agents, delegates, representatives or Subcontractors; (ii) a violation of HIPAA by Business Associate, its agents, delegates, representatives or Subcontractors; and (iii) a breach of this Agreement by Business Associate, its agents, representatives or Subcontractors. Upon demand by Covered Entity, Business Associate shall defend any investigation, claim, litigation, or other proceeding brought or threatened against Covered Entity, at Business Associate's expense, by counsel acceptable to Covered Entity. Business Associate shall not enter into any settlement without the written consent of Covered Entity. This Article V(a) shall survive the expiration or termination of this Agreement for any reason.

b. The Parties to this Agreement do not intend to create any rights in any third parties. The obligations of Business Associate under this Section and Section IV(c) of this Agreement shall survive the expiration, termination, or cancellation of this Agreement, the Service Agreement, and/or the business relationship of the Parties, and shall continue to bind Business Associate, its agents, employees, contractors, successors, and assigns as set forth herein.

c. This Agreement may be amended or modified only in a writing signed by the Parties. No Party may assign its respective rights and obligations under this Agreement without the prior written consent of the other Party. None of the provisions of this Agreement are intended to create, nor will they be deemed to create any relationship between the Parties other than that of independent parties contracting with each other solely for the purposes of effecting the provisions of this Agreement and any other agreements between the Parties evidencing their business relationship. This Agreement shall be governed by the laws of the State of New York. No change, waiver or discharge of any liability or obligation hereunder on any one or more occasions shall be deemed a waiver of performance of any continuing or other obligation, or shall prohibit enforcement of any obligation, on any other occasion. The Parties agree that, in the event that any documentation of the arrangement pursuant to which Business Associate provides Underlying Services to Covered Entity contains provisions relating to the use or disclosure of Protected Health Information which are more restrictive than the provisions of this Agreement, the provisions of the more restrictive documentation will control. The provisions of this Agreement are intended to establish the minimum requirements regarding Business Associate's use and disclosure of Protected Health Information. This Agreement, together with the Underlying Services Agreement, constitutes the entire

agreement of the Parties relating to Business Associate's use or disclosure of Protected Health Information.

d. The terms of this Agreement to the extent they are unclear, shall be construed to allow for compliance by Covered Entity with HIPAA and the HITECH Act. In the event that any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this Agreement will remain in full force and effect. In addition, in the event Covered Entity believes in good faith that any provision of this Agreement fails to comply with the then-current requirements of HIPAA, Covered Entity shall notify Business Associate in writing. For a period of up to thirty (30) days, the Parties shall address in good faith such concern and amend the terms of this Agreement, if necessary to bring it into compliance. If, after such thirty-day period, the Agreement fails to comply with the requirements of HIPAA, then Covered Entity has the right to terminate upon written notice to the Business Associate.

e. Business Associate understands and agrees that it will not assign, delegate, or subcontract any of its rights or obligations under this Agreement to individuals or entities residing outside the United States.

f. This Agreement may be executed in counterparts, each of which will constitute an original and all of which will be one and same document.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the Effective Date.

BUSINESS ASSOCIATE		**THE TRUSTEES OF COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK**	
Signature	_____	Signature	_____
Print Name	_____	Print Name	Karen Pagliaro-Meyer
Title	_____	Title	Chief Privacy Officer
Date	_____	Date	_____
Company Name	_____	Department	_____
Company Address	_____	Contact	_____
Email Address	_____		
Telephone#	_____		
Type of Business	_____		