BUSINESS ASSOCIATE AGREEMENT

This BUSINESS ASSOCIATE AGREEMENT ("BAA") is entered into this ____ day of _____, 20___, by and among The Trustees of Columbia University in the City of New York ("Columbia"), Cornell University for its Weill Cornell Medicine ("Cornell"), The New York and Presbyterian Hospital ("NYP") and _____ ("Contractor").

RECITALS

A. Columbia, Cornell and NYP are covered entities under the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA") and the HIPAA Rules (as defined below).

B. Columbia, Cornell and NYP have formed an organized health care arrangement (as defined by the HIPAA Rules). Columbia, Cornell and NYP shall be referred to herein individually as a "OHCA Member" and collectively as "OHCA."

C. OHCA intends to disclose to Contractor and to have Contractor receive or access certain Protected Health Information ("PHI"), as defined in Article 1 of this BAA, in order for Contractor to provide certain services to OHCA (the "Services") in accordance with one or more current and future agreements between the parties (the "Agreements"). The parties anticipate that Contractor will be required to create, receive, maintain, or transmit such PHI in order to provide the Services to OHCA in accordance with the Agreements. In the event of a conflict between the terms of the Agreements and the terms of this BAA, the provisions of this BAA shall prevail.

D. Contractor is a "Business Associate" under the HIPAA Rules when acting in its capacity as a service provider under the Agreements. The HIPAA Rules include the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule" at 45 CFR Part 160 and Part 164, Subparts A and E), the Standards for Security of Electronic Protected Health Information (the "Security Rule" at 45 CFR Parts 160 and 164, Subpart C), Breach Notification for Unsecured Protected Health Information (the "Breach Notification Rule" at 45 CFR Parts 160 and 164), and the Enforcement Rules at 45 CFR Part 160, Subparts C-E, as each of the foregoing may be amended or supplemented. Contractor shall adhere to the applicable requirements for Business Associates established in the HIPAA Rules.

NOW, THEREFORE, the parties, in consideration of the mutual agreements herein contained and for other good and valuable consideration, the receipt and adequacy of which are hereby acknowledged, do hereby agree as follows:

ARTICLE 1: DEFINITIONS

1.1 **Definitions.** For the purposes of this BAA, the following terms shall have the meaning as defined in the HIPAA Rules: Breach, Business Associate, Covered Entity, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use. The following terms shall have the meanings set forth below.

a. **"Administrative Safeguards"** are administrative actions, policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect Electronic PHI and to manage the conduct of the Covered Entity's or Business Associate's workforce in relation to the protection of that information.

b. **"Electronic Media"** shall mean the mode by which any electronic transfers of information are made. It includes the Internet, an intranet, an extranet, leased lines, dial-up-lines, private networks, and those transfers that are physically moved from one location to another using any data storage device, cloud storage, or other media.

c. **"Electronic PHI"** shall mean PHI that is received or transmitted by or maintained in any Electronic Media.

d. **"Physical Safeguards**" are physical measures, policies, and procedures to protect a Covered Entity's or Business Associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

e. **"Technical Safeguards"** shall mean the technology used by a Covered Entity or Business Associate to protect and control access to Electronic PHI and the policies and procedures related thereto.

ARTICLE 2: DUTIES OF CONTRACTOR REGARDING USE AND DISCLOSURE OF PHI

2.1 **Purpose.** The purpose of this BAA is for Contractor to provide the satisfactory assurances required by HIPAA and the HIPAA Rules and to further define the parties' rights and responsibilities for the exchange of PHI.

2.2 **Receipt and Use of PHI.** Satisfactory performance of its obligations under the Agreements by Contractor will require Contractor to create, receive, maintain and/or transmit PHI obtained from OHCA and/or other sources. Contractor shall not use PHI except as permitted or required by this BAA or as permitted or Required By Law. Contractor may use PHI, consistently with the HIPAA Rules: (i) for Contractor's proper internal management and administration, and (ii) to carry out the legal responsibilities of Contractor. In all instances, Contractor's use of PHI shall be consistent with minimum necessary requirements in the HIPAA Rules.

2.3 **Disclosure of PHI.** Contractor shall not disclose PHI except as expressly permitted or required by this BAA, the Agreements, or as permitted or Required By Law. Contractor shall make permissible disclosures of PHI consistent with the HIPAA Rules. Specifically, unless otherwise permitted by the Agreements or this BAA, Contractor may disclose PHI only (i) for Contractor's proper internal management and administration, or (ii) to carry out the legal responsibilities of Contractor. In either such case, Contractor shall make no such disclosure unless: (a) the disclosure is Required By Law; or (b) Contractor obtains reasonable assurances from the person to whom Contractor discloses the PHI that the PHI will be held confidentially, that the information will be used or further disclosed only as Required By Law or for the purposes for which it was disclosed, and that the person receiving such disclosure covenants that it shall notify Contractor as Required By Law of any instances of which it is or becomes aware that the confidentiality of the PHI has been Breached. In all instances, Contractor's disclosure of PHI shall be consistent with minimum necessary requirements and subject to the reproductive healthcare protections set forth in the HIPAA Rules.

2.4 **Safeguarding PHI.** Contractor shall use appropriate Administrative Safeguards, Physical Safeguards and Technical Safeguards to prevent the use or disclosure of PHI other than as permitted by this BAA. Contractor shall maintain an appropriate level of security with regard to all personnel, systems, and administrative processes used by Contractor to transmit, store, process, or otherwise handle PHI. Contractor shall not transmit PHI over any open network

unless the transmission is encrypted or otherwise secured according to the appropriate standard of care. Accordingly, Contractor 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 OHCA 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; and (iii) require that any agent or Subcontractor to whom Contractor delegates any function or activity it has undertaken to perform on behalf of OHCA, and to whom Contractor provides Electronic PHI received from, or created or received by Contractor on behalf of OHCA, agrees to implement reasonable and appropriate safeguards to protect such Electronic PHI. Further, to the extent that Contractor conducts any Transaction (as defined in 45 CFR 160.103) electronically on behalf of OHCA, it will comply with the applicable requirements in the Standards for Electronic Transactions under 45 CFR Parts 160 and 162.

2.5 **Third Party Agreements.** Under certain circumstances, Contractor may need to enter into agreements with third parties, including Subcontractors, in order to satisfy its obligations under the Agreements. Contractor shall enter into business associate agreements with all Subcontractors as required by the HIPAA Rules. Contractor shall require all of its employees, agents, as well as its Subcontractors, to whom it delegates any Services to be performed for OHCA under the Agreements, including creation, receipt, maintenance or transmission of PHI, and to whom Contractor furnishes any PHI, to agree in writing to be bound, and to abide in all respects by, all the obligations of Contractor under the HIPAA Rules, the Agreements and this BAA to protect PHI, including, but not limited to, the obligations to implement reasonable and appropriate safeguards to protect PHI and comply with the Security Rule.

2.6 **Reporting of Unauthorized Uses and Disclosures.** Contractor shall promptly (but in no case later than fifteen (15) days after discovery) notify the applicable OHCA Member(s) in writing upon becoming aware of any use or disclosure of PHI by Contractor, its employees, agents or Subcontractors that is not provided for in this BAA and any Security Incident involving PHI obtained from that OHCA Member(s). For purposes of this paragraph 2.6, "OHCA Member" shall refer to the relevant institution's Privacy Officer. In addition, in accordance with the requirements of the HIPAA Rules, Contractor shall notify the applicable OHCA Member(s) in writing of all Breaches of Unsecured PHI as soon as feasible after becoming aware of the Breach. Within ten (10) business days after becoming aware of the Breach of Unsecured PHI, Contractor shall provide to the applicable OHCA Member(s) in writing the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Contractor to have been accessed, acquired, or disclosed during such Breach. Such identification shall include a description of the Unsecured PHI involved in the Breach and all demographic information in Contractor's possession necessary to notify the affected Individuals of the Breach.

In the event of an unauthorized use or disclosure of Unsecured PHI resulting from the actions or inactions of Contractor, its agents, Subcontractors or employees, Contractor shall be responsible for, and without regard to any limitation or exclusion of damages provision set forth in any other agreement, reimbursement or direct payment of fines, penalties, and interest imposed by a governmental authority on the OHCA Member(s), and for the costs and expenses incurred by the OHCA Member(s) arising out of or related to the unauthorized use or disclosure of PHI, including but not limited to, for: (a) identifying and notifying patients whose PHI was used or disclosed, including costs related to call center support to provide information to affected individuals, (b) hiring counsel and/or auditors to investigate and report on the nature and extent of the release of Unsecured PHI; and (c) taking other reasonable measures for mitigation of harm to affected individuals, including, but not limited to, providing credit and ID theft monitoring.

Without limitation of the foregoing, Contractor shall defend, indemnify and hold harmless the affected OHCA Member(s), and their respective trustees, officers, faculty, employees and students, against any investigations, claims, litigations or other proceedings brought or threatened, and all resulting damages, losses, judgments, settlements, and liabilities (including legal fees, disbursements and costs of investigation) arising out of or relating to unauthorized use or disclosure of Unsecured PHI resulting from the actions or inactions of Contractor, its agents, Subcontractors or employees, without regard to any limitation or exclusion of damages provision set forth in any other agreement. Counsel shall be acceptable to the affected OHCA Member(s), in the exercise of its reasonable judgment. Contractor shall not enter into any settlement that admits liability or fault on the part of the OHCA Member(s) without the written consent of the affected OHCA Member(s).

In consultation with the affected OHCA Member(s), Contractor shall promptly seek to cure or mitigate, to the extent practicable, any harmful effects of an unauthorized use or disclosure of Unsecured PHI that are either known to Contractor or may reasonably be anticipated. If Contractor is unable or unwilling to promptly cure or mitigate the effects of such unauthorized use or disclosure, such inability or unwillingness shall constitute a material breach of the Contractor's obligations under this BAA, notwithstanding any other provision in the Agreements or this BAA, and OHCA shall have the right in its sole and absolute discretion to terminate for cause one or more of the Agreements to which this BAA relates. The obligations of Contractor under this Section 2.6 shall survive the termination of this BAA.

2.7 **Access to Information.** Within ten (10) business days of OHCA's written request, Contractor shall provide OHCA with access to PHI in Contractor's possession, if such PHI is contained in a Designated Record Set, in accordance with the requirements of 45 CFR 164.524.

2.8 **Availability of PHI for Amendment by Patient.** The parties acknowledge that the Privacy Rule permits an Individual who is the subject of PHI to request certain amendments of his or her records. Within ten (10) business days of a written request by OHCA for the amendment of PHI contained in a record regarding an Individual maintained by Contractor in a Designated Record Set, Contractor shall provide such information to OHCA for amendment, and Contractor shall incorporate any such amendments in the PHI as required by 45 CFR 164.526. In the event Contractor receives a request for amendment directly from an Individual or Individual's designee, Contractor shall inform OHCA of such request within ten (10) business days and respond to the Individual and incorporate the amendment, if it is acceptable, within thirty (30) days of receiving the request. Contractor shall concurrently send a copy of the response to OHCA.

2.9 **Accounting of Disclosures.** Upon OHCA's written request, Contractor shall make available to OHCA information concerning Contractor's disclosure of PHI that is required for OHCA to provide an Individual with an accounting of disclosures as required by the Privacy Rule, in accordance with 45 CFR 164.528. For this purpose, Contractor shall retain a record of disclosures of PHI for at least six (6) years from the date of disclosure. For purposes of this provision, disclosure shall include any access to the PHI by Contractor, its employees, agents and Subcontractors. In the event Contractor receives a request for an accounting of disclosures directly from an Individual or Individual's designee, Contractor shall inform OHCA of such request within ten (10) business days and respond to the Individual and provide the accounting of disclosures in accordance with the applicable HIPAA Rules. Contractor shall concurrently send a copy of the response to OHCA.

2.10 **Availability of Books and Records.** Contractor shall make its internal practices, books, and records available to the Secretary for purposes of determining the applicable OHCA Member's compliance with the Privacy Rule.

2.11 **Return of PHI at Termination.** Upon termination of the Agreements or completion of the Services, Contractor shall, where feasible, destroy or return to the applicable OHCA Member all PHI received from that OHCA Member, or created, maintained, or received by Contractor on behalf of that OHCA Member that Contractor maintains in any form. Where return or destruction is not feasible, the duties of Contractor under this BAA shall be extended to protect the PHI retained by Contractor. Contractor agrees not to further use or disclose information for which the return or destruction is infeasible. Contractor shall certify in writing the destruction of the PHI and to the continued protection of PHI that is not feasible to destroy. The obligations of Contractor under this Section 2.11 shall survive the termination of this BAA.

ARTICLE 3: TERM AND TERMINATION

3.1 **Basic Term.** This BAA shall be effective, and the parties' performance of their respective obligations under this BAA shall commence, as of the date it is executed by the parties and shall continue in effect until the later of (i) completion of the Services by Contractor, (ii) Contractor has returned or destroyed all PHI and certified thereto to OHCA as provided under Section 2.11, above, (iii) termination by the parties upon mutual written agreement; or (iv) termination pursuant to Section 3.2.

3.2 **Termination for Material Breach.** A material breach of any provision of this BAA which is not resolved within thirty (30) days of written notice to the breaching party is grounds for termination for cause under the provisions of the Agreements. The dispute resolution provisions of each respective Agreement shall apply to any disagreement between the parties as to whether Contractor has materially breached this BAA or failed to cure such breach: provided, however, the non-breaching party maintains its right to terminate the Agreement(s) notwithstanding the commencement of the dispute resolution process.

ARTICLE 4: MISCELLANEOUS

4.1 **Change in Laws.** The parties agree to negotiate in good faith if, in either party's business judgment, modification of this BAA becomes necessary due to legislative, regulatory, or judicial developments regarding HIPAA, the HIPAA Rules, or other privacy laws, rules or regulations.

4.2 **Incorporation by Reference.** The terms and provisions of HIPAA and the HIPAA Rules are incorporated herein by reference as if set forth herein at length. To the extent any provision thereof is not specifically set forth herein, such provision shall be deemed a part of this BAA and to the extent there shall be any inconsistency between the terms and provisions hereof and those set forth in HIPAA or the HIPAA Rules, the provisions of HIPAA and/or the HIPAA Rules shall prevail.

4.3 **Interpretation, Integration, Amendment.** Paragraph titles are for convenience only, and shall not be used in interpreting this BAA. This BAA contains the entire agreement of the parties and replaces all BAAs between the parties, as well as any prior conversations, notes or writings previously made with respect to the subject matter hereof, and shall not be modified or amended except in writing signed by the parties hereto.

4.4 **Counterparts.** This BAA may be executed in counterparts that, together, shall constitute one and the same BAA.

4.5 **Attorney's Fees.** If any action is brought to enforce the terms of this Business Associate Agreement, the prevailing party shall be entitled to recover its reasonable attorneys' fees, costs and expenses from the other party, in addition to any other relief to which the prevailing party may be entitled.

IN WITNESS WHEREOF, each party has caused this Business Associate Agreement to be executed and delivered by its duly authorized representative as of the date first stated above.

Contractor:

Signature: _____

Name: _____

Title: _____

The Trustees of Columbia University in the City of New York

Signature: _____

Name: _____

Title: _____

Cornell University for its Weill Cornell Medicine

Signature: _____

Name: _____

Title: _____

The New York and Presbyterian Hospital

Signature: _____

Name: _____

Title: _____