

University of North Carolina at Chapel Hill BUSINESS ASSOCIATE AGREEMENT

This Agreement is made effective the ____ of _____, 201__, by and between the University of North Carolina at Chapel Hill, on behalf of its _____, hereinafter referred to as

“Covered Entity”, and _____, hereinafter referred to as “Business Associate” (individually, a “Party” and collectively, the “Parties”). This Agreement supersedes any previously executed Business Associate Agreement between the parties.

WITNESSETH:

WHEREAS, Sections 261 through 264 of the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, known as “the Administrative Simplification provisions,” direct the Department of Health and Human Services to develop standards to protect the security, confidentiality and integrity of health information; and

WHEREAS, pursuant to the Administrative Simplification provisions, the Secretary of Health and Human Services issued regulations modifying 45 CFR Parts 160 and 164 (the “HIPAA Security and Privacy Rule”); and

WHEREAS, the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), pursuant to Title XIII of Division A and Title IV of Division B, called the “Health Information Technology for Economic and Clinical Health” (“HITECH”) Act, provides modifications to the HIPAA Security and Privacy Rule (hereinafter, all references to the “HIPAA Security and Privacy Rule” are deemed to include all amendments to such rule contained in the HITECH Act and any accompanying regulations, and any other subsequently adopted amendments or regulations); and

WHEREAS, the Parties wish to enter into or have entered into an arrangement whereby Business Associate will provide certain services to Covered Entity, and, pursuant to such arrangement, Business Associate may be considered a “business associate” of Covered Entity as defined in the HIPAA Security and Privacy Rule (the agreement evidencing such arrangement is entitled _____

_____, dated _____, and is hereby referred to as the “Arrangement Agreement”); and

WHEREAS, Business Associate may have access to Protected Health Information (as defined below) in fulfilling its responsibilities under such arrangement;

THEREFORE, in consideration of the Parties’ continuing obligations under the Arrangement Agreement, compliance with the HIPAA Security and Privacy Rule, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, and intending to be legally bound, the Parties agree to the provisions of this Agreement in order

to address the requirements of the HIPAA Security and Privacy Rule and to protect the interests of both Parties.

I. DEFINITIONS

Except as otherwise defined herein, any and all capitalized terms in this Agreement shall have the definitions set forth in the HIPAA Security and Privacy Rule. In the event of an inconsistency between the provisions of this Agreement and mandatory provisions of the HIPAA Security and Privacy Rule, as amended, the HIPAA Security and Privacy Rule shall control. Where provisions of this Agreement are different from those mandated in the HIPAA Security and Privacy Rule, but are nonetheless permitted by the HIPAA Security and Privacy Rule, the provisions of this Agreement shall control.

The term "Protected Health Information" (PHI) means individually identifiable health information including, without limitation, all information, data, documentation, and materials, including without limitation, demographic, medical and financial information, that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. "Protected Health Information" includes, without limitation "Electronic Protected Health Information," as defined below.

The term "Electronic Protected Health Information" means Protected Health Information that is transmitted by Electronic Media (as defined in the HIPAA Security and Privacy Rule) or maintained in Electronic Media.

Business Associate acknowledges and agrees that the following Protected Health Information shall be subject to this Agreement, regardless of the form of such Protected Health Information (paper record, oral communication, audio recording, or electronic display): Protected Health Information that is created or received by Covered Entity and disclosed or made available by Covered Entity or its operating units to Business Associate; and Protected Health Information that is created or received by Business Associate on Covered Entity's behalf.

II. CONFIDENTIALITY AND SECURITY REQUIREMENTS

A. Business Associate agrees:

1. to use or disclose any Protected Health Information solely: (1) for meeting its obligations as set forth in any agreements between the Parties evidencing their business relationship or (2) as required by applicable law, rule or regulation, or by an accrediting or credentialing organization to whom Covered Entity is required to disclose such information, or as otherwise permitted under this Agreement, the Arrangement Agreement (if consistent with this Agreement and the HIPAA Security and Privacy Rule), or the HIPAA Security and Privacy Rule, and (3) as would be permitted by the HIPAA Security and Privacy Rule if such use or disclosure were made by Covered Entity. All such uses and disclosures shall be subject to the limits set forth in 45 CFR § 164.514 regarding limited data sets and 45 CFR § 164.502(b) regarding the minimum necessary requirements;

2. at termination of this Agreement, the Arrangement Agreement (or any similar documentation of the business relationship of the Parties), or upon request of Covered Entity, whichever occurs first, Business Associate, if feasible, will return or destroy all Protected Health Information received from or created or received by Business Associate on behalf of Covered Entity that Business Associate still maintains in any form and retain no copies of such information. If such return or destruction of Protected Health Information is not feasible, Business Associate will extend the protections of this Agreement to the Protected Health Information and limit further uses and disclosures to those purposes that make the return or destruction of the Protected Health Information not feasible;
3. to provide HIPAA training to its personnel as appropriate to maintain the confidentiality and security of Covered Entity's records and as required by HIPAA. Business Associate may access Covered Entity's training materials online at [Information Privacy & Security Training \(http://www.unc.edu/hipaa/Annual%20HIPAA%20Training%20current.pdf\)](http://www.unc.edu/hipaa/Annual%20HIPAA%20Training%20current.pdf) then print and sign the [acknowledgment form \(http://www.unc.edu/hipaa/trainingacknowledgement2.pdf\)](http://www.unc.edu/hipaa/trainingacknowledgement2.pdf), to be kept on file at the University;
4. to ensure that its agents, including but not limited to subcontractors, to whom Business Associate provides Protected Health Information received from or created by Business Associate on behalf of Covered Entity, agree to the same restrictions and conditions that apply to Business Associate with respect to such Protected Health Information, and agree to implement reasonable and appropriate safeguards to protect such Protected Health Information that is Electronic Protected Health Information. In addition, Business Associate agrees to take reasonable steps to ensure that its employees' actions or omissions do not cause Business Associate to breach the terms of this Agreement;
5. Business Associate shall report to Covered Entity any use or disclosure of Protected Health Information that is not in compliance with the terms of this Agreement of which it becomes aware. Business Associate shall report to Covered Entity any Security Incident of which it becomes aware. For purposes of this Agreement, "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. Business Associate shall, following the discovery of a Security Incident, including that of unsecured PHI, as defined in the HITECH Act or accompanying regulations, notify the covered entity of such Incident pursuant to the terms of 45 CFR § 164.410 and cooperate in the Covered Entity's Security Incident analysis procedures, including risk assessment, if requested. A Security Incident shall be treated as discovered by Business Associate as of the first day on which such Incident is known to Business Associate or, by exercising reasonable diligence, would have been known to Business Associate, including any person, other than the person committing the Incident, who is an employee, officer, or other agent of Business Associate. Business Associate shall provide such notification to Covered Entity without unreasonable delay and in no event later than forty-eight (48) hours after discovery of the Security Incident. Such notification will contain the elements required in 45 CFR § 164.410, to the extent they are available. If the elements required in 45 CFR § 164.410 are not immediately known upon discovery of a Security Incident, Business Associate shall not delay notification of

the Incident to the Covered Entity, but instead shall provide any information that is then known and shall supplement notice to the Covered Entity promptly as more information becomes available; and

6. Business Associate will, pursuant to the HITECH Act and its implementing regulations, comply with all additional applicable requirements of the Privacy Rule, including those contained in 45 CFR §§ 164.502(e) and 164.504(e)(1)(ii), at such time as the requirements are applicable to Business Associate. Business Associate will not directly or indirectly receive remuneration in exchange for any PHI, subject to the exceptions contained in the HITECH Act, without a valid authorization from the applicable individual. Business Associate will not engage in any communication that might be deemed to be “marketing” under the HITECH Act. In addition, Business Associate will, pursuant to the HITECH Act and its implementing regulations, comply with all applicable requirements of the Security Rule, contained in 45 CFR §§ 164.308, 164.310, 164.312 and 164.316, at such time as the requirements are applicable to Business Associate.
- B. Notwithstanding the prohibitions set forth in this Agreement, Business Associate may use and disclose Protected Health Information as follows:
1. if necessary, for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided that as to any such disclosure, the following requirements are met:
 - a) the disclosure is required by law; or
 - b) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it 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, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached;
 2. for data aggregation services, if to be provided by Business Associate for the health care operations of Covered Entity pursuant to any agreements between the Parties evidencing their business relationship. For purposes of this Agreement, data aggregation services means the combining of Protected Health Information by Business Associate with the protected health information received by Business Associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.
- C. Business Associate will implement appropriate safeguards to prevent use or disclosure of Protected Health Information other than as permitted in this Agreement. Business Associate will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any Electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of Covered Entity, as required by the HIPAA Security and Privacy Rule.
- D. The Secretary of Health and Human Services shall have the right to audit Business Associate’s records and practices related to use and disclosure of Protected Health Information to ensure Covered Entity’s compliance with the terms of the HIPAA Security and Privacy Rule.

- E. Business Associate shall indemnify and hold harmless Covered Entity for any injury or damages arising from any noncompliance or Security Incident attributable to the negligence of Business Associate, including the failure to execute the terms of this Agreement. In addition, 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.

III. AVAILABILITY OF PHI

Pursuant to Section 164.522 of the HIPAA Security and Privacy Rule, Business Associate agrees to comply with any requests for restrictions on certain disclosures of Protected Health Information to which Covered Entity has agreed and of which Business Associate is notified by Covered Entity. Consistent with Section 164.524 of the HIPAA Security and Privacy Rule, Business Associate agrees to make available Protected Health Information; provided, however, that Business Associate, upon request for Protected Health Information, shall provide such Protected Health Information to Covered Entity, and Covered Entity shall make such Protected Health Information available to the applicable individual. If Business Associate maintains Protected Health Information electronically, it agrees to make such Protected Health Information electronically available to Covered Entity, which will make such Protected Health Information available to the applicable individual. Business Associate agrees to make Protected Health Information available for amendment and incorporate any amendments to Protected Health Information in accordance with the requirements of Section 164.526 of the HIPAA Security and Privacy Rule. In addition, Business Associate agrees to make Protected Health Information available for purposes of accounting of disclosures, as required by Section 164.528 of the HIPAA Security and Privacy Rule and Section 13405(c)(3) of the HITECH Act. Business Associate and Covered Entity shall cooperate in providing any accounting required on a timely basis.

IV. TERMINATION

Notwithstanding anything in this Agreement to the contrary, Covered Entity shall have the right to terminate this Agreement and the Arrangement Agreement immediately if Covered Entity determines that Business Associate has violated any material term of this Agreement. If Covered Entity reasonably believes that Business Associate will violate a material term of this Agreement and, where practicable, Covered Entity gives written notice to Business Associate of such belief, and Business Associate within a reasonable period of time after receiving such notice and in any event before the threatened breach is to occur, fails to provide adequate written assurances to Covered Entity that it will not breach the cited term of this Agreement, then Covered Entity shall have the right to seek an injunction enjoining Business Associate from violating this Agreement or to unilaterally terminate this Agreement and the Arrangement Agreement immediately.

V. MISCELLANEOUS

Except as expressly stated herein or in the HIPAA Security and Privacy Rule, the Parties to this Agreement do not intend to create any rights in any third parties. The obligations of Business Associate under this Section shall survive the expiration, termination, or cancellation of this Agreement, the Arrangement 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.

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 will be governed by the laws of the State of North Carolina. 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 services to Covered Entity contains provisions relating to the use or disclosure of Protected Health Information that 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.

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. To the extent any changes in the HIPAA Security and Privacy Rule, including any then-current requirements of the HITECH Act or its regulations, conflict with the terms and conditions of this Agreement, such changes shall have the full force and effect of law and supersede the terms and conditions of this Agreement. Notwithstanding the fact that changes in the law shall supersede any conflicting terms of this Agreement, in the event a Party believes in good faith that any provision of this Agreement fails to comply with the then-current requirements of the HIPAA Security and Privacy Rule, including any then-current requirements of the HITECH Act or its regulations, such Party shall notify the other Party in writing. For a period of up to thirty 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 HIPAA Security and Privacy Rule, including the HITECH Act, then either Party has the right to terminate upon written notice to the other Party.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the day and year written above.

COVERED ENTITY:

BUSINESS ASSOCIATE:

University of North Carolina at Chapel Hill,
On behalf of its _____

By: _____

By: _____

Printed Name: _____

Printed Name: _____

Title: _____

Title: _____

Agreement renews or expires on: _____

SAMPLE