BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is entered between the University of North Carolina Greensboro _____ ("Covered Entity" or "CE" or "UNCG") and _____ ("Business Associate" or "BA"), collectively "the Parties," who agree as follows:

Explanatory Statement

BA shall supply CE with the following services: _____ (the "Services") that require the use and/or disclosure by CE of Protected Health Information as herein defined. These Services are provided pursuant to a "Services Agreement" between the Parties, and this Agreement shall be incorporated as an integral part of the Services Agreement. In connection with those services, Business Associate will have access to certain information that is subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing privacy and security regulations at 45 Code of Federal Regulations ("C.F.R.") Parts 160-164 ("HIPAA Privacy Rule" and "HIPAA Security Rule" or "HIPAA Privacy & Security Rule"), the applicable provisions of Article 39, Chapter 57 of the North Carolina General Statutes, and the Family Educational Rights and Privacy Act ("FERPA").

The parties acknowledge that this Business Associate Agreement (the "Agreement") is required by the Privacy Rules promulgated pursuant to the regulations issued in connection with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") as amended, and incorporates the requirements of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") that are applicable to business associates, along with any guidance and/or regulations issued by the U.S. Department of Health and Humans Services ("DHHS"). The BA recognizes and agrees that it is obligated by law to meet the applicable provisions of the HITECH Act.

Agreement

Now, therefore, in consideration of the premises and of the mutual promises herein contained, and the Explanatory Statement, which is made a substantive part hereof, the parties hereto agree as follows:

1. Definitions.
    a. Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in 45 C.F.R. Parts 160, 162 and 164.

    b. Catch-All Definition:
        i. The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, 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.

    c. Specific Definitions:
        i. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164.

ii. "Individual" shall have the same meaning as the term "individual" in 45 C.F.R. § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

iii. "Privacy Rule" shall mean the federal privacy regulations at 45 C.F.R. § 160 and subparts A and E of 45 C.F.R. § 164.

iv. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. § 160 and subparts A and C of 45 C.F.R. § 164.

v. "PHI" shall mean Protected Health Information, as defined in 45 C.F.R. § 160.103, limited to the Protected Health Information received from, or received or created on behalf of, CE by BA pursuant to the Agreement. e-PHI or ePHI refers to "electronic Protected Health Information" and shall also mean Protected Health Information. The HIPAA Security Rule establishes national standards to protect individuals' e-PHI that is created, received, used, or maintained by a HIPAA covered entity.

vi. "Required by Law" shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.103.

vii. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his or her designee.

viii. "Subsequent Recipient" shall mean any person to whom BA discloses PHI, including, without limitation, agents and subcontractors of BA.

2. Obligations and Activities of BA. BA agrees to:

a. Not use or disclose PHI other than as permitted or required by the Agreement or as required by law;

b. Use appropriate safeguards, and comply with Subpart C or C.F.R. § 164 with respect to ePHI, to (i) prevent use or disclosure of PHI other than as permitted or required by this Agreement; (ii) reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI that it creates, maintains, or transmits on behalf of the CE; and (iii) comply with those requirements set forth in 45 C.F.R.. §§ 164.308, 164.310, 164.312, and 164.316 that are applicable to BA; Where the BA does not comply with the Security or Privacy Rule, provide CE with a Plan of Action and Milestones for remediation within 30 calendar days. CE and its authorized representatives shall have the right to audit, to examine, and request compliance artifacts pertaining to the BA's compliance with the Privacy Rule and Security Rule. This includes, but is not limited to those policies, procedures, and documented safeguards implemented by the BA, its employees, agents, assigns, successors, and subcontractors. The BA shall at any time as requested by the CE, whether during or after completion of this Agreement, and at BA's own expense make such compliance artifacts available for inspection and audit;

c. Promptly report to CE any use or disclosure of PHI not permitted by the Services Agreement of which it becomes aware, including breaches of unsecured PHI as required at 45 C.F.R. § 164.410, and any security incident of which it becomes aware;

d. Without unreasonable delay, and in no case later than seven (7) calendar days after discovery, BA shall notify CE of a Breach of any Secured PHI or any Unsecured PHI all in accordance with 42 U.S.C. § 17932(b) and 45 C.F.R. § 164.410;

e. In accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors, agents and Subsequent Recipients that create, receive, maintain, or transmit PHI on behalf of the BA agree, in writing, to the same restrictions, conditions and requirements that apply to the BA with respect to such information; promptly notify in writing if BA changes any of the subcontractors or agents that create, receive, maintain, or transmit PHI. This also includes notifying the CE if the BA, or the BA's subcontractors or agents change ownership (e.g. bought or sold, merged);

f. Make available, and provide upon request, in a designated record its internal practices, books, and records relating to the use and disclosure of PHI to the Secretary as necessary to satisfy the CE's obligations under 45 C.F.R. § 164.524;

g. Within thirty (30) days after receiving a written request from CE, make available information necessary for CE to make an accounting of disclosures of PHI about an Individual as provided in 45 C.F.R. § 164.528 and 42 U.S.C. § 17935(c), and when directed by CE, make that accounting directly to the Individual;

h. Mitigate, to the extent practicable, any harmful effect that is known to BA of a use or disclosure of PHI by BA that is not permitted by the requirements of this B.A. Agreement;

i. Provide access (at the request of the CE, and in the time and manner designated by CE) to PHI in a Designated Record Set, to CE or, as directed by CE, to an Individual, in accordance with the requirements of 45 C.F.R. § 164.524;

j. In the event that BA in connection with the Services uses or maintains an Electronic Health Record of information of or about an Individual, then the BA shall provide an electronic copy (at the request of CE, and in the time and manner designated by CE) of the PHI, to CE or, when and as directed by CE, to an Individual or a third party designated by the Individual, all in accordance with 42 U.S.C. § 17935(e);

k. Make available, within thirty (30) days of a written request by CE, PHI for amendment and incorporate any amendments to the PHI as directed by CE, all in accordance with 45 C.F.R. § 164.526;

l. Comply with requests for restrictions on certain disclosures of PHI pursuant to 45 C.F.R. § 164.522 to which CE has agreed and of which BA is notified by CE;

m. Request, use and/or disclose only the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure in compliance with 45 C.F.R. § 164.502(b), and comply with 45 C.F.R. § 514 regarding limited data sets;

n. Consider whether any use of disclosure of PHI can be made through "de-identified" PHI as set forth in 45 C.F.R. § 164.514(b)(2)(i) and (ii). BA agrees neither to de-identify PHI it creates or receives for or from CE or from another business associate of CE, nor use or

disclose such de-identified PHI unless (i) such de-identification is expressly permitted under the terms and conditions of an amendment to this Agreement and (ii) such de-identification is for services provided by BA that related to CE's activities for purposes of Payment of Health Care Operations. Unless expressly permitted, by written agreement, BA shall not de-identify PHI;

o. Not directly or indirectly receive remuneration in exchange for any PHI in compliance with 42 U.S.C. § 17935(d);

p. Not make or cause to be made any communication about a product or service that is prohibited by 42 U.S.C. § 17936(a);

q. Report and track all Security Incidents:
    i. BA will report to CE any Security Incident that results in the unauthorized access, Use, Disclosure, modification, or destruction of CE's ePHI or interferes with BA's system operations in BA's information systems of which BA becomes aware. BA will inform CE's Privacy Official within twenty-four (24) hours after BA learns of such non-permitted or violating Use or Disclosure, and provide a report within ten (10) days, containing information containing the nature and impact of the security incident and the steps to mitigate its impact. BA agrees to provide such other information concerning the Security Incident as requested by CE;

r. Develop and implement policies and procedures and meet the Security Rule documentation requirements. Upon CE request, will provide access to and copies of these policies and procedures; and

s. Mitigate, to the extent practicable, any harmful effect that is known to BA resulting from or that may result in a Security Incident, including, but not limited to: (i) assess BA's systems for configuration vulnerabilities and vendor patch maintenance on an ongoing basis and take reasonable steps to apply security patches and remediate any substantial vulnerabilities; (ii) cooperate with CE if CE determines that it is necessary and appropriate for BA to shut down its internet facility services provided to CE and/or cease connectivity to the service of CE's own network until CE determines that all risks have been appropriately mitigated; (iii) cooperate as reasonably requested by CE to further investigate and resolve the Security Incident; and (iv) use best efforts to prevent any further security Incident or other prohibited Use or Disclosure; however, such remedial actions shall in no manner relieve BA's obligations or liabilities for breach hereunder.

3. Access, Amendment, and Disclosure Accounting by BA
    a. BA will promptly, upon CE's request, make available to CE, or at CE's direction, to the individual or individual's personal representative for inspection and obtaining copies any PHI in a designated record set about the individual with BA created or received from CE and that is in CE's custody or control so that CE may meet its access obligations under 45 C.F.R. § 164.524. BA shall make such information available in electronic format when directed by CE.

b. BA will promptly upon CE's request amend or permit CE access to amend any portion of the PHI which BA created or received from CE, and incorporate any amendments to such PHI, so that CE may meet its amendment obligations under 45 C.F.R. § 164.526.

c. BA will record for each disclosure, not excepted from disclosure accounting under this section, that BA makes to CE or a third part of PHI that BA creates or receives for or from CE, the request set for in the HIPAA Privacy & Security Rule, including, but not limited to (i) the disclosure state, (ii) the name and if known the address of the person or entity to whom the BA made the disclosure, (iii) a brief description of the PHI disclosure, and (iv) a brief statement of the purpose of the disclosure.

d. For Repetitive disclosures made to the same person or entity (including CE) for a single purpose, BA may provide (i) the information for the first of the Repetitive disclosures, (ii) the frequency, period or number of these Repetitive disclosures and (iii) the date of the last of these disclosures.

e. BA will make Disclosure information available to CE promptly upon CE's request.

f. BA will make its internal practices, books, and records relating to its Use and Disclose of the PHI it creates or receives from CE available to DHHS to determine CE's compliance with 45 C.F.R. §§ 160 -164. At the request of the Secretary of DHHS, BA will comply with any investigations and compliance reviews, permit access to information, provide records and compliance reports, and cooperate with any complaint investigation pursuant to 45 C.F.R. § 164.130.

4. Other Permitted Uses and Disclosures by BA
    a. Specific Purposes. Except as otherwise limited in this Agreement, BA may use or disclose PHI on behalf of, or to provide services to, CE as specified in the Services Agreement, if such use or disclosure of PHI would not violate the Privacy Rule or Security Rule if done by CE.

    b. Specific Use and Disclosure Provisions.
        i. Except as otherwise limited in this Agreement, BA may disclose PHI for the proper management and administration of the BA or to carry out the legal responsibilities of the BA, provided that such disclosures are Required by Law, or BA obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and be 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 the BA of any instances of which it is aware in which the confidentiality of the information has been breached.
        ii. Except as otherwise limited in this Agreement, BA may use PHI to provide Data Aggregation services to CE as permitted by 42 C.F.R. § 164.504(e)(2)(i)(B).

5. Obligations of CE
    a. Provisions for CE to Inform BA of Privacy and Security Practices and Restrictions.
        i. CE shall provide BA with the notice of privacy and security practices that CE produces in accordance with 45 C.F.R. §§ 164.520 and 164.316, as well as any changes to such notice.

ii. CE shall provide BA with any changes in, or revocation of, permission by any Individual or Representative to use or disclose PHI, if such changes affect BA's permitted or required uses or disclosures.
iii. CE shall notify BA of any restrictions on to the use or disclosure of PHI or to which CE has agreed in accordance with 45 C.F.R. § 164.522.

b. Permissible Requests by CE. CE shall not request BA to use or disclose PHI in any manner that would not be permissible under then-current law or regulation.

6. Breach of Privacy Obligations
   a. Reporting. BA will report to CE and (i) acquisition, access, Use or Disclosure of PHI that is neither permitted by this Agreement nor given prior written approval by CE; and (ii) any Breach of Unsecured PHI. CE has sole authority to perform a risk assessment to determine whether the Breach compromises the security or privacy of the Unsecured PHI; as such BA's obligation to report shall include any Unauthorized acquisition, access, Use or Disclosure, even where BA has determined that such Unauthorized acquisition, access, Use or Disclosure does not compromise the security or privacy of such information. BA shall cooperate with CE in investing the Breach and in meeting CE's obligations under the Breach Notification Rule and any other security Breach notification laws. BA will make the report to CE's Privacy Official within ten (10) days after BA learns of such non-permitted, acquisition, access, Use or Disclosure. Said report will at a minimum:
      i. Describe the nature of the unauthorized acquisition, access, Use or Disclosure, including the date of the Breach and the Date of Discovery;
      ii. Identify each individual whose PHI has been or is reasonably believed by the BA to have been acquired, access, Used or Disclosed, including the types of identifiers and likelihood of re-identification;
      iii. Describe how Unauthorized acquisition, access, Use or Disclosure occurred, including whether the PHI was actually acquired or viewed;
      iv. Identify who made, and who received, the Unauthorized acquisition, access, Use or Disclosure;
      v. Identify what corrective action BA took or will take to prevent further Unauthorized acquisition, access, Use or Disclosure;
      vi. Identify what BA did or will do to mitigate any deleterious effect of the Unauthorized acquisition, access, Use or Disclosure and the extent to which the risk to PHI has been mitigated; and
      vii. Provide such other information as CE may reasonably request.

7. Term and Termination.
   a. *Term.* The Term of this Agreement shall be effective as of the date of full execution of this Agreement by duly authorized representatives of both Parties, and shall terminate in accordance with the termination of the Services Agreement or termination of the BA relationship between the Parties consistent with this Section, whichever is sooner.

   b. *Termination for Cause.* Upon either party's knowledge of a material breach of this Agreement by the other party, the non-breaching party may terminate this Agreement and the Services Agreement upon thirty (30) days written notice or provide the other party written notice of such breach and terminate this Agreement and the Services Agreement if

the other party does not cure the breach or end and remedy the violation within five (5) days of receipt of such notice.

c. *Termination by UNCG.* UNCG may terminate this Agreement without liability, penalty or expense in the event of non-appropriation of state funds or upon thirty (30) days prior written notice with or without cause.

d. *Obligations of BA Upon Termination.* Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, BA shall return or destroy all PHI received from CE, or created, maintained or received by BA on behalf of CE, that the BA still maintains in any form. This provision shall apply to PHI that is in the possession of subcontractors, agents and Subsequent Recipients of BA. BA shall retain no copies of the PHI.

   i. In the event that BA determines that returning or destroying the PHI is infeasible, BA shall provide to CE notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return, or destruction of PHI is infeasible, BA shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible.

e. *Survival.* The obligations of BA under this Section shall survive the termination of this Agreement.

8. Miscellaneous

a. *Regulatory References.* A reference in this Agreement to a section of a statute regulation or rule means the section as in effect or as amended, and for which compliance is required.

b. *Amendment.* The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules, ARRA and their rules and regulations, including, but not limited to, the Privacy Rules. This Agreement may be amended only in a writing signed by both Parties.

c. *Interpretation.* Any ambiguity in this Agreement shall be interpreted to permit compliance with HIPAA, Privacy and Security Rules.

d. *Effect of Instrument Under Seal.* This document is an instrument under SEAL and, as such, it is the Parties intention that the longest possible period of limitations pursuant to North Carolina's applicable Statute of Limitations shall apply to this Agreement.

e. *Rights of Third Parties.* This Agreement is between BA and CE and shall not be construed, interpreted, or deemed to confer any rights whatsoever to any third party or parties.

f. *Indemnification.* BA shall indemnify, defend, and hold harmless CA, its Trustees, officers, agents, and employees from all loss, cost, and expense in connection with or arising out of any liability or claim of liability for injury or damages to persons or property sustained or claimed to have been sustained by anyone whomsoever, by reason of the performance of this Agreement, or by any act or omission of BA or any of its officers, agents, employees, guests, patrons, or invitees.

g. *Compliance Monitoring.* BA agrees to cooperate with CE's Privacy Official during the conduct of a business associate privacy compliance review. Cooperation shall include, but is not limited to, the right to visit a site, and/or providing prompt access to or copies of BA's privacy policies, procedures and other documentation as may be reasonably requested that relate to BA's handling of PHI.

h. *Applicable Law.* The law of North Carolina shall be applied in interpreting this Agreement.

i. *Family Educational Rights and Privacy Act (FERPA).* The parties have determined that BA is a school official with a legitimate educational interest under FERPA. If CE provided BA with (i) "personally identifiable information" from a student's education record as defined by FERPA, 34 C.F.R. § 99 or (ii) personal identifying information as defined in N.C. Gen. Stat. § 132-1.10 (collectively, "Confidential Information") BA hereby certifies that collection of this Confidential Information is necessary for the performance of its duties and responsibilities on behalf of CE. BA certifies that it shall maintain the confidential and exempt status of the Confidential Information in its custody, and that it shall not re-disclose Confidential Information as directed by FERPA and other applicable state and federal laws. If BA experiences a security breach relating to Confidential information or BA re-discloses the Confidential Information the BA shall immediately notify the CE. BA shall indemnify CE for any breach of confidentiality or failure of its responsibilities to protect the Confidential Information. Specifically, these costs may include, but are not limited to, the cost of notification of affected persons as a result of its release. Failure to abide by legally applicable security measures and disclosure restrictions may result in the interruption, suspension, and/or termination of the relationship between CE and BA for a period of at least five years from the date of violation.

j. *Dispute Resolution.* Any lawsuit between the parties arising from this Agreement shall be filed solely in a court of competent jurisdiction in Guilford County, North Carolina.

k. *Assignment.* No Party may assign its rights or duties hereunder without the written consent of the other Party.

l. *Legal Compliance.* Both Parties agree to comply with all applicable Federal and North Carolina laws including, but not limited to, non-discrimination on the basis of race, sex, religion, national origin, age, handicap or sexual orientation.

IN WITNESS THEREOF, the parties have executed this Agreement effective the day and year first written below.

The University of North Carolina Greensboro	_____ Name of Company or Individual
By: _____	By: _____
Print Name: _____	Print Name: _____
Title: _____	Title: _____
Date:_____	Date:_____