CREDIBILITY • INTEGRITY • ACHIEVEMENT

HIPAA BUSINESS ASSOCIATE ADDENDUM

This Business Associate Addendum (the "Addendum") is effective upon execution, and amends and is made part of the Accreditation Agreement dated as of _____ by and between the Council on Accreditation ("Business Associate") and_____ ("Organization") (including all addenda, exhibits, amendments, other documents, and service plans incorporated therein, the "Accreditation Agreement").

WITNESSETH:

WHEREAS, Organization is seeking accreditation by the Council on Accreditation; and,

WHEREAS, Organization wishes, in furtherance of the accreditation process, to allow the Council on Accreditation, including members of its staff and its volunteers, which shall include but not be limited to Reviewers and Accreditation Commissioners, its officers and directors, and members of its board of directors (hereinafter collectively, "COA"), to have access to Protected Health Information or Electronic Protected Health Information, as such term is defined in 45 CFR Parts 160, 162, and 164 (the "Privacy and Security Rules") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XII of Division A, and Title IV of Division B of the American Recovery and Reinvestment Act (ARRA) of 2009 that is either provided to COA by Organization in the course of performing the Accreditation Services or during maintenance of accreditation hereinafter set forth; and,

WHEREAS, COA requires access to such Protected Health Information in order to effectively perform the Accreditation Services; and,

WHEREAS, Organization is a Covered Entity as such term is defined by the Privacy and Security Rules promulgated pursuant to the 45 CFR Parts 160, 162, and 164 (the "Privacy and Security Rules") under HIPAA and is required by the Privacy and Security Rules to obtain satisfactory assurance from its Business Associates with respect to maintaining the confidentiality of Protected Health Information accessed, used, or disclosed by its Business Associates on behalf of Organization; and,

WHEREAS, COA is a Business Associate of Organization.

NOW THEREFORE, Organization and COA mutually agree to modify the Accreditation Agreement to incorporate the terms of this Addendum in order to set forth the terms and

conditions pursuant to which the Protected Health Information will be handled by COA and certain third parties, as applicable, for the duration of the Accreditation Agreement and upon its termination, cancellation, or expiration in order to comply with the requirements of the HIPAA Privacy and Security Rules.

1. DEFINITIONS

1.1 Business Associate. "Business Associate" ("BA") shall have the meaning set forth in 45 CFR 160.103, as such provision is currently drafted and as it is subsequently updated or revised.

1.2 Breach. Means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the Privacy Rule that compromises the security or privacy of the Protected Health Information. For purpose of this definition, "compromises the security or privacy of the Protected Health Information" means poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of Protected Health Information that does not include the identifiers listed in 164.514(e)(2), limited data set, date of birth, and zip code does not compromise the security or privacy of the Protected Health Information.

Breach excludes:

A. Any unintentional acquisition, access, or use of Protected Health Information by a workforce member or person acting under the authority of a BA if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

B. Any inadvertent disclosure by a person who is authorized to access Protected Health Information at a BA to another person authorized to access Protected Health Information at the same BA, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.

C. A disclosure of Protected Health Information where the BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

1.3 Covered Entity. "Covered Entity" ("CE") shall have the meaning set forth in 45 CFR 160.103, as such provision is currently drafted and as it is subsequently updated or revised.

1.4 Designated Record Set. "Designated Record Set" shall have the meaning set forth in 45 CFR 164.501, as such provision is currently drafted and as it is subsequently updated or revised.

1.5 Disclosure. "Disclosure" or "Disclose" shall mean the release, transfer, provision of access to, or divulging in any other manner of information outside of the entity holding the information.

1.6 HHS. "HHS" shall mean the Department of Health and Human Services.

1.7 Individual. "Individual" shall have the same meaning as the term "individual" set forth in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in

accordance with 45 CFR 164.502(g), as such provisions are currently drafted and as they are subsequently updated or revised.

1.8 Privacy Officer. "Privacy Officer" shall have the meaning set forth in 45 CFR 164.530(a)(1), as such provision is currently drafted and as it is subsequently updated or revised.

1.9 Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information as set forth in 45 CFR Parts 160 and 164 (as amended, modified or superseded from time to time).

1.10 Required by Law. “Required by Law” shall have the same meaning as the term “required by law” in 45 CFR 164.501.

1.11 Security Rule. “Security Rule” shall mean Security Standards for the protection of Electronic Protected Health Information as set forth in 45 CFR Parts 160, 162, and 164 (as amended, modified or superseded from time to time).

1.12 Protected Health Information. “Protected Health Information” (“PHI”) shall mean individually identifiable health information that is: transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium. PHI includes demographic information unless such information is de-identified according to the Privacy Rule. PHI includes without limitation “Electronic Protected Health Information” as defined below.

1.13 Electronic Protected Health Information. “Electronic Protected Health Information” (“EPHI”) shall mean protected health information that is transmitted by Electronic Media (as defined in the HIPAA Privacy and Security Rules) or maintained in Electronic Media.

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

1.15 Security Incident. “Security Incident” shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. An attempted unauthorized access means any attempted unauthorized access that prompts the BA to investigate the attempt, or review or change its current security measures.

1.16 Use. “Use” shall mean the sharing, employment, application, utilization, examination, or analysis of PHI within the entity that maintains such information.

1.17 Unauthorized. “Unauthorized” is an impermissible use or disclosure of PHI under the HIPAA Privacy Rule.

1.18 Unsecured Protected Health Information: PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L.111-5 on the HHS website.

2. Capitalized terms used, but not otherwise defined, in the Accreditation Agreement or this Addendum shall have the meaning set forth in the Privacy and Security Rules.

3. Prohibition on Unauthorized Use or Disclosure of PHI. BA shall not use or disclose any PHI received from or on behalf of the CE except as permitted or required by the Accreditation Agreement or this Addendum to provide accreditation services to the CE in accordance with its accreditation policies and procedures, as published in the *COA Accreditation Policies and Procedures Manual*, as updated from time to time (the "Accreditation Procedures") and which are incorporated into this Addendum by reference, and in accordance with the terms and conditions set forth in the Accreditation Agreement (the "Accreditation Services"), as required by law, or as otherwise authorized in writing by the CE. Except as otherwise provided herein, BA may use or disclose PHI only as necessary to satisfy its obligations under the Accreditation Agreement to provide Accreditation Services, which include, for example, reviewing self-studies, determining compliance with standards, and reporting suspected abuses to the appropriate governmental entities or authorities, as specified by its accreditation policies and procedures or as otherwise permitted by law; and to comply with applicable state and federal law and regulations as long as such use or disclosure of PHI would not violate the Privacy and Security Rules if done by CE.

4. Use of PHI for BA's Operations. BA may use and/or disclose PHI it accesses or receives from CE to the extent necessary for BA's proper management and administration, or to carry out its legal responsibilities, only if:

A. The disclosure is required by law to maintain its status as an approved accreditor; or,

B. BA obtains reasonable assurances, evidenced by written contract, from any person or organization to which BA shall disclose such PHI that such person or organization shall:

i. Hold such PHI in confidence and use or further disclose it only for the purpose for which BA disclosed it to the person or organization, or as required by law; and,

ii. Notify BA, who shall in turn promptly notify CE, of any occurrence that the person or organization becomes aware of in which the confidentiality of such PHI was breached.

5. Safeguarding of PHI. BA shall develop, implement, maintain, and use reasonable and appropriate administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of all PHI, in any form or media, accessed, received, or maintained on behalf of CE. BA shall document and keep these security measures current. BA shall cooperate in good faith in response to any reasonable requests from CE to discuss, review, inspect, and/or audit BA's safeguards.

6. Subcontractors and Agents. If BA provides any PHI that was received from CE to a subcontractor or agent, then BA shall require such subcontractor or agent to agree in writing to the same restrictions and conditions as are imposed on BA by this Addendum.

7. Access to PHI. Within a reasonable time of receipt of written request from CE, BA agrees to provide access to any PHI held by BA that CE has determined to be part of CE's Designated Record Set, in the time and manner designated by CE. This access will be provided to CE or, as directed by CE, to an Individual, in order to meet the requirements under the Privacy Rule.

8. Amendment or Correction to PHI. Within a reasonable time of receipt of written request from CE, BA agrees to amend or correct PHI held by BA, which CE has determined to be part of CE's Designated Record Set, in the time and manner designated by CE.

9. Reporting of an Incident/Breach, Unauthorized Disclosures, or Misuse of PHI (Occurrence). BA shall report within ten (10) business days to the CE's Privacy Officer or, if no Privacy Officer has been appointed, other designated personnel as indicated in the signature block of this addendum, a discovery of breach or any use or disclosure of PHI that is not in compliance with the terms of this Addendum, including those occurrences reported to BA by its subcontractors or agents. An occurrence of PHI shall be treated as "discovered" as of the first day on which such occurrence is known to BA, or, by exercising reasonable diligence would have been known to the BA. The report from BA to CE shall include the following:

i. The name of each individual whose PHI has been or is reasonably believed to have been accessed, acquired, or disclosed during the occurrence.

ii. A brief description of what happened, including the date of the occurrence and the date of the discovery of the occurrence, if known.

iii. A description of the types of PHI that were involved in the occurrence (such as full name, social security number, date of birth, home address, account number, etc.).

iv. A brief description of what BA is doing to investigate the occurrence, to mitigate losses, and to protect against further occurrences.

v. The actions BA has undertaken or will undertake to mitigate any harmful effect of the occurrence.

vi. A corrective action plan that includes the steps the BA has taken or shall take to prevent future similar occurrences.

10. Mitigating Effect of an Incident/Breach, Unauthorized Disclosures, or Misuse of PHI. BA agrees to mitigate, to the extent practicable, any harmful effect that is known to BA of a misuse or unauthorized disclosure of PHI by BA in violation of the requirements of this Addendum. The BA shall reasonably cooperate with CE's efforts to seek appropriate injunctive relief or otherwise prevent or curtail such threatened or actual breach, or to recover its PHI, including complying with a reasonable Corrective Action Plan.

11. Tracking and Accounting of Disclosures. So that CE may meet its accounting obligations under the Privacy Rule. Within a reasonable time of receipt of a written request from CE, BA agrees to provide it with the information necessary to allow CE to respond to a request for an accounting of disclosures in accordance with 45 CFR 164.528.

A. Disclosure Tracking. For each disclosure of PHI that BA makes to a third party that is not excepted under subsection (b) below, BA will record (i) the disclosure date, (ii) the name and (if known) address of the person or entity to whom BA made the disclosure, (iii) a brief description of the PHI disclosed, and (iv) a brief statement of the purpose of the disclosure. For repetitive disclosures that BA makes to the same person or entity for a single purpose, BA may provide (i) the disclosure information for the first of these repetitive disclosures, (ii) the frequency, periodicity, or number of these repetitive disclosures, and (iii) the date of the last of these repetitive disclosures. BA will make this log of disclosure information available to the CE within five (5) business days of the CE's request.

B. Exceptions from Disclosure Tracking. Business Associate need not record disclosure information or otherwise account for disclosures of PHI if:

i. The disclosures are permitted under this Addendum, or are expressly authorized by Covered Entity in another writing; and,

ii. The disclosures are for one of the following purposes:
a. Treatment, Payment, or Health Care Operations unless § 14.D., below, applies;
b. In response to a request from the Individual who is the subject of the disclosed PHI, or to that Individual's Personal Representative;
c. Made to persons involved in that individual's health care or payment for health care;
d. For notification for disaster relief purposes;
e. For national security or intelligence purposes;
f. As part of a Limited Data Set or,
g. To law enforcement officials or correctional institutions regarding inmates.

C. Disclosure Tracking Time Periods. Business Associate must have available for Covered Entity the disclosure information required by this section for the six-year

period preceding Covered Entity's request for the disclosure information.

12. Accounting to CE and to Government Agencies. BA shall make its internal practices, books, and records relating to the use and disclosure of PHI received from CE available to CE, or at the request of CE or the Secretary of the Department of Health and Human Services (HHS), to the Secretary of the Department of Health and Human Services (HHS) or his/her designee, in a time and manner designated by CE or the Secretary or his/her designee, for the purpose of determining CE's compliance with the Privacy Rule. BA shall promptly notify CE of communication with HHS regarding PHI provided or created by CE and shall provide CE with copies of any information BA has made available to HHS under this provision.

13. Term and Termination.

A. This Addendum shall take effect upon execution.

B. In addition to the rights of the parties established by the underlying Accreditation Agreement, if CE reasonably determines in good faith that BA has materially breached any of its obligations under this Addendum, CE, in its sole discretion, shall have the right to:

i. Exercise any of its rights to reports, access and inspection under this Addendum; and/or

ii. Require BA to submit to a plan of monitoring and reporting, as CE may determine necessary to maintain compliance with this Addendum; and/or

iii. Provide BA with a thirty (30) day period to cure the breach; or

iv. Terminate the Agreement immediately.

C. Before exercising any of these options, CE shall provide written notice to BA describing the violation and the action it intends to take.

14. Return or Destruction of PHI. Upon termination, cancellation, expiration, or other conclusion of the Agreement, BA shall:

A. Return to CE or, if return is not feasible, destroy all PHI in whatever form or medium it was received from CE. This provision shall also apply to all PHI that is in the possession of subcontractors or agents of BA. In such case, BA shall retain no copies of such information, including any compilations derived from and allowing identification of PHI. BA shall complete such return or destruction as promptly as possible, but not more than thirty (30) days after the effective date of the conclusion of the Agreement. Within such thirty (30) day period, BA shall certify on oath in writing to CE that such return or destruction has been completed.

B. If BA destroys PHI, it shall be done with the use of technology or methodology that

renders the PHI unusable, unreadable, or undecipherable to unauthorized individuals as specified by HHS in HHS guidance. Acceptable methods for destroying PHI include: (i) paper, film, or other hard copy media shredded or destroyed in order that PHI cannot be read or reconstructed; and (ii) electronic media cleared, purged, or destroyed consistent with the standards of the National Institute of Standards and Technology (NIST). HHS specifically excludes redaction as a method of destruction of PHI, unless the information is properly redacted so as to be fully de-identified.

C. If BA believes that the return or destruction of PHI is not feasible, BA shall provide written notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction is not feasible, BA shall extend the protections of this Addendum to PHI received from or used on behalf of CE, and limit further uses and disclosures of such PHI, for so long as BA maintains the PHI.

15. Responsibilities of CE. CE hereby undertakes to do the following:

A. Immediately inform BA of any changes in CE's Notice of Privacy Practices (the "Notice") that CE provides to Individuals pursuant to 45 CFR 164.520, and provide BA a current copy of such Notice and a copy of all updated versions thereof prior to their effective date.

B. Immediately notify BA in writing of any substitution of the Privacy Officer or other designated personnel.

C. Immediately inform BA of any changes in, or withdrawal of, any relevant authorization provided to CE by Individuals pursuant to 45 CFR 164.508.

D. Immediately notify BA, in writing, of any arrangements permitted or required under 45 CFR parts 160 and 164 or other applicable law that may have any impact whatsoever on the use and/or disclosure of PHI by BA under the Accreditation Agreement, including, but not limited to, restrictions on use and/or disclosure of PHI as provided for in 45 CFR 164.522 agreed to by CE.

E. Immediately notify COA in writing of any restrictions that CE has agreed to adhere to with regard to the use and disclosure of PHI of any Individual that materially affects and/or limits the uses and disclosures that are otherwise permitted by this Addendum.

16. Miscellaneous.

A. Automatic Amendment. Upon the effective date of any amendment to HIPAA and the Privacy and Security Rules promulgated by HHS with regard to PHI, this Addendum shall automatically amend so that the obligations imposed on BA and CE remain in compliance with such regulations.

B. Interpretation. Any ambiguity in this Addendum shall be resolved in favor of a meaning that permits CE and BA to comply with HIPAA.

C. De-Identification of Information. At certain points in the accreditation process, BA requests that CE provide BA with information in a non-identified or de-identified format. CE assumes full responsibility that either such documentation does not contain PHI, or that it is in fact de-identified, as requested, and BA assumes no responsibility for any unauthorized use and/or disclosure of PHI that occurs as a result of CE's failure to thoroughly de-identify such information. Where the Accreditation Agreement grants BA the right to disclose "non-identifying information" to third parties for the purpose of Research Studies, BA assumes responsibility for de-identifying such information, to the extent that it constitutes PHI, prior to any such disclosure.

D. Information That Does Not Qualify as PHI De-Identified Information. The restrictions on BA's use and disclosure of information, and the obligations on BA created by this Addendum do not apply with respect to information received or generated by BA from or on behalf of CE that is not PHI, or that is converted by BA into de-identified information. BA may use and disclose such information, as provided in the Accreditation Agreement, to perform data aggregation, or for comparative studies for its own use. The results of any such data aggregation or other comparative studies shall be the sole property of BA. CE shall have no rights, and BA shall have no obligations or duties to CE with respect to such information.

IN WITNESS WHEREOF, each of the undersigned has caused this Addendum to be duly executed in its name and on its behalf effective as of _____, _____(the "Effective Date").

(insert organization name above)

By:_____

Print Name:_____

Title: _____

Date:_____

Council on Accreditation

By:_____

Print Name:_____

Title: _____

Date:_____

PRIVACY OFFICER OR OTHER DESIGNATED PERSONNEL

Name: _____

Contact Information:

_____

_____