HIPAA BUSINESS ASSOCIATE ADDENDUM

This Addendum amends and is hereby incorporated into the existing Purchase of Service Agreement No. **Contract #** ("Agreement"), entered into by and between the County of Dane (hereinafter referred to as "COUNTY") and **Provider legal entity** (hereinafter "PROVIDER").

COUNTY and PROVIDER mutually agree to modify the Agreement to incorporate the terms of this Addendum to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 ("HITECH"), and HIPAA's implementing regulations, Title 45, Parts 160 and 164 of the Code of Federal Regulations ("Security and Privacy Rules"), as amended, dealing with the security, confidentiality, integrity and availability of Protected Health Information as well as breach notification requirements. If any conflict exists between the terms of the original Agreement and this Addendum, the terms of this Addendum shall govern.

This Addendum is specific to those services and programs included in the Agreement in which PROVIDER may create, access, receive, maintain or transmit Protected Health Information on behalf of COUNTY and where it has been concluded that PROVIDER is performing specific functions on behalf of COUNTY that have been determined to be covered under the HIPAA Security and Privacy Rules. PROVIDER's activities within the Agreement may include, but are not limited to the following: (i) claims processing or administration, (ii) data analysis, processing or administration, (iii) utilization review, (iv) quality assurance, (v), billing, (vi) benefit management, (vii) practice management, (viii) other management or administrative functions, including legal, actuarial, accounting, consulting, or data management functions, or (ix) where PROVIDER is a health provider not otherwise subject to the Security and Privacy Rules, including other health service functions. PROVIDER is responsible for securely maintaining Protected Health Information on behalf of COUNTY, and for complying with the HIPAA Security and Privacy Rules, including, but not limited to breach notification rules, to the same extent as COUNTY.

1. Definitions:
   a. Protected Health Information (PHI) means any information, unless excluded from protection under the Security and Privacy Rules, whether oral or recorded in any form or medium, including Electronic Health Records, that: (i) relates to the past, present or future physical or mental condition of any Individual; the provision of health care to an Individual; or the past, present or future payment of the provision of health care to an Individual; and (ii) identifies the Individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the Individual. PHI includes demographic information.
   b. Individual means the person who is the subject of PHI, and shall include a person who qualifies under the Security and Privacy Rules as a personal representative of the Individual.
   c. Breach means the unauthorized acquisition, access, use or disclosure of Unsecured PHI in a manner not permitted under the Privacy Rule that creates a significant risk of financial, reputational or other harm to the Individual.

d. Unsecured Protected Health Information means PHI that is not rendered unusable, unreadable or indecipherable through the use of technology or methodology specified by the U.S. Secretary of Health and Human Services ("Secretary") that compromises the security or privacy of the PHI. Unsecured PHI is presumed to be compromised unless following a risk assessment that fairly considers the nature and extent of the breach and potential injury to affected Individuals, it is determined that the PHI has not been compromised.

e. 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.

f. Capitalized terms used in this Addendum, but not otherwise defined, shall have the same meaning as those terms in the Security and Privacy Rules, as amended.

2. Prohibition on Unauthorized Use or Disclosure of PHI: PROVIDER shall not access, transmit, maintain, retain, modify, record, store, destroy, hold, use or disclose any PHI received from or on behalf of COUNTY except as permitted or required by the Agreement or this Addendum, as required by law, or as otherwise authorized in writing by COUNTY.

3. Use and Disclosure of Protected Health Information: PROVIDER may create, use or disclose PHI only for the following purposes:
   a. For the proper management and administration of the functions and activities related to the provision of healthcare services specified within the Purchase of Services Agreement.
   b. For meeting its obligations as set forth in any agreements between the parties evidencing their business relationship.
   c. As would be permitted by the Security and Privacy Rules if such use or disclosure were made by COUNTY or as required by applicable law, rule or regulation.
   d. For Data Aggregation purposes for the Health Care Operations of COUNTY.
   e. For use in PROVIDER's operations as outlined in paragraph 4. below.

   Disclosures of PHI shall, to the extent practicable, be limited to the applicable limited data set and to the minimum necessary information to accomplish the intended purpose of the use, disclosure or request.

4. Use of PHI for PROVIDER's Operations: PROVIDER may use and/or disclose PHI it creates for, or receives from, COUNTY to the extent necessary for PROVIDER's proper management and administration, or to carry out PROVIDER's legal responsibilities, only if:
   a. The disclosure is required by law, and only to the extent required by law.
   b. PROVIDER obtains reasonable assurances, evidenced by written contract, from any person or organization to which PROVIDER 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 PROVIDER disclosed it to the person or organization, or as required by law; and
      (ii) Agree to the same restrictions and conditions as imposed on PROVIDER by this Addendum.

(iii) Notify PROVIDER, who shall in turn promptly notify COUNTY, of any Security Incident or Breach of PHI.

c. PROVIDER keeps COUNTY informed of the identities of all such persons or organizations having access to PHI created, received, maintained or transmitted on behalf of COUNTY.

5. Notice of Privacy Practices: For the purpose of PHI created or maintained for COUNTY covered by this Agreement, PROVIDER will not maintain Notice of Privacy Practices providing less protection than stated in COUNTY's Notice of Privacy Practices.

6. Safeguarding of PHI: PROVIDER shall develop, implement, maintain, use and regularly review appropriate administrative, technical, and physical safeguards to protect the confidentiality, integrity and availability of all PHI, in any form or media, including electronic storage and transmission, received from, created, received, maintained or transmitted by PROVIDER on behalf of COUNTY. PROVIDER will maintain policies and procedures to protect against the identity theft of client/consumer information. PROVIDER shall document, periodically review and keep these security measures current, consistent with the Security and Privacy Rules. PROVIDER shall cooperate and respond in good faith to any reasonable request from COUNTY to discuss and review PROVIDER's safeguards.

7. Subcontractors and Agents. If PROVIDER provides any PHI received from, created or maintained on behalf of COUNTY to a subcontractor or agent, PROVIDER shall require in writing the same safeguards and restrictions no less stringent than required by this Addendum. PROVIDER will also inform such subcontractors and agents that they are subject to the Security and Privacy Rules by virtue of this Addendum.

6. Compliance with Electronic Transactions and Code Set Standards: If PROVIDER conducts any Standard Transaction for, or on behalf, of COUNTY, PROVIDER shall comply, and shall require any subcontractor or agent conducting such Standard Transaction to comply, with each applicable requirement of Title 45, Part 162 of the Code of Federal Regulation. PROVIDER shall not enter into, or permit its subcontractors or agents to enter into, any Agreement in connection with the conduct of Standard Transactions for or on behalf of COUNTY that:

a. Changes the definition, Health Information condition, or use of a Health Information element or segment in a Standard.

b. Adds any Health Information elements or segments to the maximum defined Health Information Set.

c. Uses any code or Health Information elements that are either marked "not used" in the Standard's Implementation Specification(s) or are not in the Standard's Implementation Specifications(s).

d. Changes the meaning or intent of the Standard's Implementations Specification(s).

7. Access to PHI: At the direction of COUNTY, PROVIDER agrees to provide access to PHI held by PROVIDER which COUNTY has determined to be part of COUNTY's Designated Record Set, in the time and manner designated by COUNTY. This access will be provided to COUNTY or, upon advance notice to COUNTY, to an Individual, in order to meet the requirements under the Security and Privacy Rules.

8. Amendment or Correction to PHI: At the direction of COUNTY, PROVIDER agrees to amend or correct PHI held by PROVIDER and which COUNTY has determined to be part of COUNTY's Designated Record Set, in the time and manner designated by COUNTY.

9. Reporting of Security Incidents Involving PHI: PROVIDER shall report to COUNTY the discovery of any Breach of or Security Incident involving PHI. PROVIDER shall make the report to COUNTY's Privacy Official not less than one (1) business day after PROVIDER learns of such Breach or Security Incident. PROVIDER's report of a Breach shall identify as applicable: (i) each individual protected by the Agreement whose PHI has been, or is reasonably believed by PROVIDER to have been breached, accessed, acquired or disclosed, (ii) the nature of the unauthorized use or disclosure, (iii) the PHI used or disclosed, (iv) who made the unauthorized use or received the unauthorized disclosure, (v) PROVIDER's risk analysis of financial, reputational or other harm that may result, (vi) what PROVIDER has done or shall do to mitigate any deleterious effect of unauthorized use or disclosure, (vii) what notifications PROVIDER has or shall make resulting from a Breach of Unsecured PHI, and (viii). what corrective action PROVIDER has taken or shall take to prevent future similar unauthorized use or disclosure. PROVIDER shall provide such other information, including a written report, as reasonably requested by COUNTY's Privacy Official.

10. Mitigating Effect of Unauthorized Disclosure or Misuse of PHI: PROVIDER agrees to mitigate, to the extent practicable, any harmful effect that is known to PROVIDER of a Breach, including, if necessary, payment of the cost of credit monitoring. PROVIDER will cooperate with COUNTY's efforts to seek corrective and mitigation actions.

11. Notification Requirements In Event of Unauthorized Disclosure or Misuse of PHI received, maintained or transmitted on behalf of COUNTY: PROVIDER agrees, at its own cost and after obtaining consultation and agreement from COUNTY, to no later than 60 days following a Breach to:
    a. Provide written notice to the Individual or next of kin if the Individual is deceased, as required by law.
    b. If contact information is insufficient to provide notice to an individual, provide a substitute form of notice; and, where there are 10 or more Individuals with insufficient contact information, make a conspicuous posting as required by the Secretary as provided on the Secretary's official web site.
    c. If breach involves the PHI of more than 500 Individual residents of the state, notify prominent media outlets.
    d. Include in notice to Individuals: (i) a brief description of what happened; (ii) a description of the type of information involved; (iii) steps Individuals should take to protect themselves from potential harm resulting from the Breach; a description of what is being done to investigate the Breach, mitigate losses and protect against further breaches; and (iv) contact procedures for Individuals to obtain further information.
    e. Comply with any other notice requirements of the Security and Privacy Rules, or guidance statements of the Secretary, as from time to time amended.
    f. Reporting all actions taken to COUNTY.

12. Log of Unauthorized Disclosure or Misuse of PHI: PROVIDER shall maintain a log of any Breach of PHI covered by this Addendum and shall annually submit such log to the Secretary and to COUNTY. PROVIDER shall provide immediate notice to the Secretary and COUNTY of any breach of the PHI of 500 or more Individuals.

13. Tracking and Accounting of Disclosures: So that COUNTY may meet its accounting obligations under the Security and Privacy Rules,
    a. Disclosure Tracking. Unless excepted under subsection (b) below, PROVIDER will record for each disclosure of PHI it makes that PROVIDER creates or receives for or from COUNTY (i) the disclosure date, (ii) the name and (if known) address of the person or entity to whom PROVIDER 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 which PROVIDER makes to the same person or entity, including the COUNTY, for a single purpose, PROVIDER 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. PROVIDER will make this log of disclosure information available to the COUNTY within five (5) business days of the COUNTY's request.
    b. Disclosure Tracking Time Periods. PROVIDER must have available for the Individual and COUNTY the disclosure information required by this section for the six-year period preceding the request for the three-year period preceding a request for the disclosures of Electronic Health Records made for purpose of Treatment, Payment and Health Care Operations.

14. Accounting to COUNTY and to Government Agencies: PROVIDER shall make its internal practices, books, and records relating to the use and disclosure of PHI received from or on behalf of or created for COUNTY available to COUNTY, or at the request of COUNTY, to the Secretary or his/her designee, in a time and manner designated by COUNTY or the Secretary or his/her designee, for the purpose of determining COUNTY's compliance with the Security and Privacy Rules. PROVIDER shall promptly notify COUNTY of communications with the Secretary regarding PHI provided by or created by COUNTY and shall provide COUNTY with copies of any information PROVIDER has made available to the Secretary under this provision.

15. Prohibition on Sale of Protected Health Information: PROVIDER shall not receive remuneration in exchange for any PHI of an Individual received from or on behalf of COUNTY.

16. Response to Subpoena: In the event that PROVIDER receives a subpoena or similar requirement for the production of PHI received from, or created on behalf of COUNTY, PROVIDER shall promptly forward a copy of such subpoena to the Director of the Dane County Department of Human Services to afford COUNTY the opportunity to timely respond to the demand for its PHI as COUNTY determines appropriate.

17. Termination:

    In addition to the rights of the parties established by the underlying Agreement, if COUNTY reasonably determines in good faith that PROVIDER has materially

breached any of its obligations under this Addendum, COUNTY, in its sole discretion, shall have the right to:

a. Exercise any of its rights to reports, access and inspection under this Addendum; and/or
b. Require PROVIDER to submit to a plan of monitoring and reporting, as COUNTY may determine necessary to maintain compliance with this Addendum, and/or
c. Provide PROVIDER with a reasonable period to cure the breach; or
d. Terminate the Agreement immediately.

18. Return or Destruction of PHI: Upon termination, cancellation, expiration or other conclusion of PROVIDER's contractual relationship with COUNTY, PROVIDER shall:
    a. Return to COUNTY or, if return is not feasible, destroy all PHI and all Health Information in whatever form or medium that PROVIDER received from or created on behalf of COUNTY. This provision shall also apply to all PHI that is in the possession of subcontractors or agents of PROVIDER. In such case, PROVIDER shall retain no copies of such information, including any compilations derived from and allowing identification of PHI. PROVIDER shall complete such return or destruction as promptly as possible, but not less than thirty (30) days after the effective date of the conclusion of PROVIDER's contractual relationship with COUNTY. Within such thirty- (30) day period, PROVIDER shall certify on oath in writing to COUNTY that such return or destruction has been completed.
    b. If PROVIDER destroys PHI, it shall render the PHI completely unusable, unreadable, and undecipherable to unauthorized persons using approved methods. Electronic redaction is an insufficient method of destruction.
    c. If PROVIDER believes that the return or destruction of PHI is not feasible, upon mutual agreement of the Parties, PROVIDER shall extend the protections of this Addendum to PHI received from or created on behalf of COUNTY, and limit further uses and disclosures of such PHI, for so long as PROVIDER maintains the PHI.

19. Miscellaneous:
    a. Automatic Amendment. Upon the effective date of any amendment to the regulations promulgated by the Secretary with regard to PHI, this Addendum shall automatically amend so that the obligations imposed on PROVIDER remain in compliance with such regulations.
    b. Interpretation. Any ambiguity in this Addendum shall be resolved in favor of a meaning that permits COUNTY to comply with the Security and Privacy Rules.
    c. Indemnification. PROVIDER shall defend and hold COUNTY harmless from all costs, including attorney fees, resulting from PROVIDER’s failure to meet any of its obligations under this Addendum.
    d. Independent Contractor Status. Nothing in this Agreement shall be interpreted to alter PROVIDER’s independent contractor status with COUNTY.

IN WITNESS WHEREOF, the undersigned has caused this Addendum to be duly executed in its name and on its behalf.

For PROVIDER:

By: _____

_____

(Print or type name)

Title:_____

Date:_____