

Business Associate Agreement

This **AGREEMENT** is made between:

Covered Entity

Kewaunee County
Department of Human Services
810 Lincoln Street
Kewaunee, WI 54216

Primary Contact:
Human Services Director
(920) 388-7030
Fax - (920) 388-7044

Business Associate

Provider Name
Address
Address
Address

Primary Contact:
Name, Title
Telephone
Fax
Email

This Agreement is effective January 1, 2014 and shall terminate on December 31, 2014.

RECITALS

- A. Covered Entity and Business Associate entered into an agreement (the "Underlying Agreement") pursuant to which Business Associate agrees to perform certain services on behalf of Covered Entity.
- B. In performing services on behalf of the Covered Entity, Business Associate may create, access, receive, maintain or transmit Covered Entity's Protected Health Information (defined below).
- C. The parties wish to enter into this Agreement to set forth their understanding with regard to Business Associate's Use and Disclosure of Protected Health Information (defined below) in accordance with the business associate agreement requirements of the Health Insurance Portability and Accountability Act of 1996, 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 all applicable implementing regulations, including, without limitation, the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule"), Notification in the Case of Breach of Unsecured Protected Health Information ("Breach Notification Rule"), and the Security Standards for the Protection of Electronic Protected Health Information (the "Security Rule") found at Title 45, Parts 160 and 164 of the Code of Federal Regulations, dealing with the security, confidentiality, integrity and availability of protected health or health-related information, as well as breach notifications (all such laws and regulations shall be collectively referred to herein as "HIPAA").

AGREEMENTS

In consideration of the Recitals and the mutual agreements which follow, Covered Entity and Business Associate agree as follows:

1. Definitions. Capitalized terms used in this Agreement, but not otherwise defined, shall have the same meaning as those terms in the Privacy Rule or the Security Rule.

(a) Breach means the acquisition, access, Use, or Disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. PHI is presumed to be compromised unless Covered Entity or Business Associate, as applicable, documents that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

- (i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- (ii) The unauthorized person who used the PHI or to the Disclosure was made;
- (iii) Whether the PHI was actually acquired or viewed; and
- (iv) The extent to which the risk to the PHI has been mitigated.

Breach excludes:

- (i) Any unintentional acquisition, access or Use of PHI by a workforce member or person acting under the authority of a Covered Entity or Business Associate 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.
 - (ii) Any inadvertent Disclosure by a person who is authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the same Covered Entity or Business Associate, or organized health care arrangement in which the Covered Entity participates, 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.
 - (iii) A Disclosure of PHI where a Covered Entity or Business Associate 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.
- (b) Protected Health Information or "PHI" means that individually identifiable health information (including ePHI as defined below) of the Covered Entity that is created, used, disclosed, maintained, or received by the Business Associate, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:
- (i) Past, present or future physical or mental health or condition of an individual

- (ii) The provision of health care to an individual
- (iii) The past, present, or future payment for the provision of health care to an individual excluding:
 - [a] Regarding a person who has been deceased for more than 50 years;
 - [b] Employment records held by Covered Entity in its role as employer;
 - [c] Education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g and student records described at 20 U.S.C. 1232g(a)(4)(B)(iv).
- (c) Electronic Protected Health Information or "ePHI" means that PHI of Covered Entity which is transmitted by Electronic Media (as defined in the HIPAA Privacy and Security Rule) or maintained in Electronic Media.
- (d) Individual means the person who is the subject of PHI, and shall include a person who qualifies under the Privacy Rule as a personal representative of the Individual.
- (e) Unsecured Protected Health Information means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a 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. <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html>

2. Responsibilities of Business Associate.

- (a) Prohibition on Unauthorized Use or Disclosure of PHI. Business Associate shall not use or disclose any PHI received from or on behalf of Covered Entity except as permitted or required by the Agreement or this Agreement, as Required by Law, or as otherwise authorized in writing by Covered Entity.
- (b) Minimum Necessary. Business Associate shall not request, use or disclose more than the minimum amount of PHI necessary to accomplish the purpose of the Use, Disclosure, or request.
- (c) Use and Disclosure of PHI. Except as described in Section 4, Business Associate may access, transmit, maintain, retain, modify, record, store, destroy or otherwise hold, use or disclose PHI only for the following purposes(s):
 - (i) *[List Business Associate's permitted uses and disclosures here, or incorporate by reference an attached Exhibit where the uses and disclosures are described.]*
- (d) Use of PHI for Business Associate's Operations. Business Associate may use and/or disclose PHI it creates for, or receives from, Covered Entity to the extent necessary for Business Associate's proper management and administration, or to carry out Business Associate's legal responsibilities, only if:
 - (i) The Disclosure is Required by Law; or

- (ii) Business Associate obtains reasonable assurances, evidenced by written contract, from any person or organization to which Business Associate shall disclose such PHI that such person or organization shall:
 - [a] hold such PHI in confidence and use or further disclose it only for the purpose for which Business Associate disclosed it to the person or organization, or as Required by Law; and
 - [b] notify Business Associate, who shall in turn promptly notify Covered Entity, of any occurrence which the person or organization becomes aware of in which there was a privacy or security incident and/or the confidentiality of such PHI was breached.

- (e) De-identification of PHI.
 - (i) Creation and Use of De-identified Data. In the event Business Associate wishes to de-identify PHI, it must first submit its proposed plan for accomplishing the conversion to Covered Entity for Covered Entity's approval, which shall not be unreasonably withheld provided such conversion meets the requirements of 45 CFR § 164.514. Business Associate may use de-identified PHI only as directed or otherwise agreed to by Covered Entity.
 - (ii) Re-identification Prohibited. Unless otherwise agreed upon by the parties, in the event that Covered Entity provides Business Associate with de-identified PHI, Business Associate shall not be given access to, nor shall Business Associate attempt to develop on its own, any keys or codes that can be used to re-identify the data.

- (f) Safeguarding of PHI.
 - (i) Business Associate shall use appropriate safeguards and comply with Subpart C of 45 CFR Part 164, Security Standards for the protection of Electronic Protected Health Information, with respect to ePHI, to prevent access, use, or disclosure of ePHI other than as provided for by this Agreement.
 - (ii) To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under the Privacy Rule, Business Associate shall comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s). This includes using appropriate safeguards to prevent inappropriate and/or unauthorized access, use, or disclosure of PHI.
 - (iii) Business Associate shall review and modify its privacy and security safeguarding measures as needed to continue providing reasonable and appropriate protection of PHI.
 - (iv) Business Associate shall maintain documentation of privacy and security safeguarding measures as required by HIPAA.

- (v) Business Associate shall cooperate in good faith in response to any reasonable requests from Covered Entity to discuss, review, inspect, or audit Business Associate's safeguards.

- (g) Subcontractors. If at any time PHI received from, or created or received by Business Associate on behalf of Covered Entity, is provided or made available by Business Associate to any of its Subcontractors, then Business Associate shall require each such Subcontractor to agree in writing to the same restrictions and conditions on the Use or Disclosure of PHI as are imposed on Business Associate by this Agreement and applicable law, including the HIPAA Privacy and Security Rules. Business Associate shall ensure that all such Subcontractors that create, receive, maintain, or transmit PHI will implement reasonable and appropriate safeguards to protect such PHI.

- (h) No Off-Shore Activities. Absent prior written approval of Covered Entity, Business Associate shall neither provide nor transmit Covered Entity's PHI, for any purpose, to any person or entity located outside the geographic boundaries of the United States, including employees, agents or other representatives of that person or entity. Absent prior written approval of Covered Entity, Business Associate shall neither provide nor facilitate access to Covered Entity's PHI for any person or entity located outside the geographic boundaries of the United States including employees, agents or other representatives of that person or entity.
 - (i) Compliance with Electronic Transactions and Code Set Standards. If Business Associate conducts any Standard Transaction for, or on behalf, of Covered Entity, Business Associate shall comply, and shall require any Subcontractor conducting such Standard Transaction to comply, with each applicable requirement of Title 45, Part 162 of the Code of Federal Regulation. Business Associate shall not enter into, or permit its Subcontractors to enter into, any Agreement in connection with the conduct of Standard Transactions for or on behalf of Covered Entity that:
 - (ii) Changes the definition, Health Information condition, or use of a Health Information element or segment in a Standard;
 - (iii) Adds any Health Information elements or segments to the maximum defined Health Information Set;
 - (iv) 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); or
 - (v) Changes the meaning or intent of the Standard's Implementations Specification(s).

- (i) Access to PHI. At the direction of Covered Entity or an Individual, Business Associate agrees to provide access to any PHI held by Business Associate, which Covered Entity has determined to be part of Covered Entity's Designated Record Set, in the time and manner designated by Covered Entity. Further, Business Associate shall grant Individuals access to an electronic copy of PHI maintained electronically in that Individual's Designated Record Set in accordance with 45 CFR § 164.524(c).

Business Associate also shall provide or transmit the copy of PHI to a third party if directed in writing to do so by the Individual or Covered Entity. This access will be provided to the Individual, Covered Entity or, as directed by Covered Entity, to an Individual, in order to meet the requirements under the Privacy Rule.

- (j) Amendment or Correction to PHI. At the direction of Covered Entity, Business Associate agrees to amend or correct PHI held by Business Associate, which Covered Entity has determined to be part of Covered Entity's Designated Record Set, in the time and manner designated by Covered Entity.
- (k) Reports of Nonpermitted Uses or Disclosures, Security Incidents or Breaches.
 - (i) Reports of Nonpermitted Use or Disclosure. Business Associate agrees to promptly report to Covered Entity any Use or Disclosure of the PHI not provided for by this Agreement and cooperate with Covered Entity in its investigation of such event.
 - (ii) Reports of Security Incidents. For purposes of this Section, "Security Incident" shall have the same meaning as "Security Incident" in 45 CFR § 164.304. Business Associate agrees to promptly notify Covered Entity of any Security Incident involving PHI of which it becomes aware and cooperate with Covered Entity in the investigation. Business Associate will report attempted but unsuccessful Security Incidents that do not result in any unauthorized access, Use, Disclosure, modification or destruction of PHI, or interference with an information system at Covered Entity's request, at least annually even in the absence of the Covered Entity's request.
 - (iii) Reports Related to Potential Breach of Unsecured PHI.
 - [a] Following the discovery of a Breach of Unsecured PHI, Business Associate shall notify Covered Entity of the Breach. Such notification shall be made without unreasonable delay after discovering the Breach, but no later than sixty (60) calendar days after its discovery.
 - [b] Business Associate's notice shall include, to the extent possible, the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used, or disclosed during or as a result of the Breach. Business Associate shall also provide Covered Entity with at least the following information: a description of the Breach, including the date of Breach and the date of discovery of the Breach, if known; a description of the types of Unsecured PHI involved in the Breach; any steps Individuals should take to protect themselves from potential harm resulting from the Breach; a brief description of what Business Associate is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any further Breaches; and any other information requested by Covered Entity related to the Breach. Business Associate shall promptly supplement such notice with additional information as it becomes available, even if such

information becomes available after Individuals have been notified of the Breach.

- [c] Business Associate agrees to cooperate with Covered Entity in the investigation of a Breach of Unsecured PHI and to cooperate with and participate in, to the extent requested by Covered Entity, the notification of Individuals, the media, and the Secretary of any Breach of Unsecured PHI.
 - [d] In the event that: (i) a Breach of Unsecured PHI occurs because of the action or inaction of Business Associate, its employees, agents, representatives, or Subcontractors; or (ii) a Breach occurs involving Unsecured PHI in Business Associate's possession, or PHI created, maintained, transmitted, or received by Business Associate or its employees, agents, representatives, or Subcontractors, Business Associate agrees that Covered Entity may, in its sole discretion, require Business Associate to provide such notification as may be required of Covered Entity by 45 CFR §§ 164.404, 164.406, and 164.408. Covered Entity shall have the right to review, direct, and approve or reject the contents or manner of such notification.
- (l) Mitigation. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of PHI by Business Associate in violation of the requirements of this Agreement.
 - (m) Tracking and Accounting of Disclosures. So that Covered Entity may meet its accounting obligations under the Privacy Rule, Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. For each Disclosure of PHI that Business Associate makes to Covered Entity or to a third party that is subject to Disclosure under 45 CFR § 164.528, Business Associate will record (i) the Disclosure date, (ii) the name and (if known) address of the person or entity to whom Business Associate 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 Business Associate makes to the same person or entity, including the Covered Entity, for a single purpose, Business Associate may provide (i) the Disclosure information for the first of these repetitive disclosures, (ii) the frequency, duration or number of these repetitive disclosures, and (iii) the date of the last of these repetitive disclosures. Business Associate will make this log of Disclosure information available to the Covered Entity within five (5) business days of the Covered Entity's request. Business Associate must retain the Disclosure information for the six-year period preceding Covered Entity's request for the Disclosure information.
 - (n) Audit. For purposes of determining Business Associate's or Covered Entity's compliance with HIPAA, upon request of Covered Entity or the Secretary of Health and Human Services, Business Associate shall: (i) make its HIPAA policies and procedures, related documentation, records maintained, and any other relevant internal practices and books relating to the Use and Disclosure of PHI, available to the Secretary of Health and Human Services or to Covered Entity and (ii) provide

reasonable access to Business Associate's facilities, equipment, hardware and software used for the maintenance or processing of PHI. Business Associate shall promptly notify Covered Entity of communications with the Secretary regarding PHI and shall provide Covered Entity with copies of any information Business Associate has made available to the Secretary under this Section 2 of the Agreement.

- (o) Response to Subpoena. In the event Business Associate receives a subpoena or similar notice or request from any judicial, administrative or other party which would require the production of PHI received from, or created for, Covered Entity, Business Associate shall promptly forward a copy of such subpoena, notice or request to Covered Entity to afford Covered Entity the opportunity to timely respond to the demand for its PHI as Covered Entity determines appropriate according to its state and federal obligations.

3. Covered Entity's Obligations.

- (a) Notice of Privacy Practices. Covered Entity shall notify Business Associate of any limitation in its Notice of Privacy Practices, to the extent such limitation affects Business Associate's permitted Uses or Disclosures.
- (b) Individual Permission. Covered Entity shall notify Business Associate of changes in, or revocation of, permission by an Individual to Use or disclose PHI, to the extent such changes affect Business Associate's permitted Uses or Disclosures.
- (c) Restrictions. Covered Entity shall notify Business Associate of any restriction in the Use or Disclosure of PHI to which Covered Entity has agreed, to the extent such restriction affects Business Associate's permitted Uses or Disclosures.
- (d) Requests. Covered Entity shall not request Business Associate to Use or disclose PHI in any manner that would not be permissible under the Privacy Rule if used or disclosed by the Covered Entity.

4. Term and Termination; Effect of Termination.

- (a) Term. This Agreement shall take effect upon the Effective Date and shall remain in effect until all PHI is returned to Covered Entity or destroyed in accordance with the terms of this Agreement.
- (b) Termination. If either party reasonably determines in good faith that the other party has materially breached any of its obligations under this Agreement, the nonbreaching party shall have the right to:
 - (i) Exercise any of its rights to reports, access and inspection under this Agreement;
 - (ii) Require the breaching party to submit to a plan of monitoring and reporting, as the nonbreaching party may determine necessary to maintain compliance with this Agreement;
 - (iii) Provide the breaching party with a ten (10) day period to cure the breach; and/or

- (iv) Terminate this Agreement immediately.
- (c) Before exercising any of these options, nonbreaching party Entity shall provide written notice to breaching party describing the violation and the action it intends to take.
- (d) Effect of Termination; Return or Destruction of PHI. Upon termination, cancellation, expiration, or other conclusion of the Agreement, Business Associate shall, and shall ensure its Subcontractors that possess PHI or data derived from PHI ("Related Data") chose and fulfill one of the following options with respect to such PHI and Related Data:
 - (i) Return PHI, and any Related Data, to Covered Entity in whatever form or medium that Business Associate received from or created on behalf of Covered Entity. In such case, no copies of such PHI and Related Data shall be retained. PHI and Related Data shall be returned as promptly as possible, but not more than thirty (30) days after the effective date of the conclusion of this Agreement or the underlying Agreement. Within such thirty (30) day period, Business Associate shall certify on oath in writing to Covered Entity that such return has been completed.
 - (ii) Destroy the PHI, and any Related Data, using technology or a methodology that renders the PHI, or Related Data, unusable, unreadable, or undecipherable to unauthorized individuals as specified by HHS in its guidance at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html>. Acceptable methods for destroying PHI or Related Data include: (A) paper, film, or other hard copy media shredded or destroyed in order that PHI or Related Data cannot be read or reconstructed; and (B) electronic media cleared, purged or destroyed consistent with the standards of the National Institute of Standards and Technology (NIST). Redaction as a method of destruction of PHI or Related Data is specifically excluded.
 - (iii) If Business Associate believes that the return or destruction of PHI or Related Data is not feasible, Business Associate shall provide written notification of the conditions that make return or destruction infeasible. If the Covered Entity agrees that return or destruction is not feasible, Business Associate shall extend the protections of this Agreement to PHI and Related Data received from or created on behalf of Covered Entity, and limit further uses and disclosures of such PHI and Related Data, for so long as Business Associate maintains the PHI. If the Covered Entity does not agree that destruction is infeasible, the Business Associate must either return or destroy the PHI.

5. Miscellaneous.

- (a) Automatic Amendment. Upon the effective date of any amendment to HIPAA, the Privacy Rule or the Security Rule promulgated by HHS with regard to PHI, this Agreement shall automatically amend so that the obligations imposed on Business Associate remain in compliance with such regulations.

- (b) Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity and Business Associate to comply with HIPAA.
- (c) Independent Contractor Status. The parties agree that in performing the Services and satisfying the obligations of this Agreement, Business Associate shall at all times be an independent contractor for Covered Entity and nothing in this Agreement shall be construed as creating an agency, employment, joint venture, partnership or other relationship. Covered Entity shall neither have nor exercise any control or direction over Business Associate. Business Associate shall avoid taking any action or making any representation or warranty whatsoever with respect to its relationship with Covered Entity which is inconsistent with its independent contractor status.
- (d) Conflicts. Any provision of the Underlying Agreement that is directly contradictory to one or more terms of this Agreement ("Contradictory Term") shall be superseded by the terms of this Agreement only to the extent of the contradiction, as necessary for the parties' compliance with HIPAA and to the extent that it is reasonably impossible to comply with both the Contradictory Term and the terms of this Agreement.
- (e) Integration. This Agreement contains the entire understanding between the parties hereto relating to the subject matter herein and shall supersede any other oral or written agreements, discussions and understandings of every kind and nature, including any provision in any services agreement.
- (f) Waiver. No delay or failure of either party to exercise any right or remedy available hereunder, at law or in equity, shall act as a waiver of such right or remedy, and any waiver shall not waive any subsequent right, obligation, or default.

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

COVERED ENTITY

BUSINESS ASSOCIATE

By: _____

By: _____

Title: _____

Title: _____

Date: _____

Date: _____