

Attachment 2

BUSINESS ASSOCIATE AGREEMENT

This Agreement is made effective Month day, year by and between Name of Office, Division or Institution (“Covered Entity”) and Name of Contractor/Business Associate (“Business Associate”) collectively the “Parties”).

1. BACKGROUND

This Agreement is specific to those services, activities, or functions performed by the Business Associate on behalf of the Covered Entity when such services, activities, or functions are covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Services, activities, or functions covered by this Agreement include, but are not limited to:

Insert description of covered services, activities for functions contracted for

The Covered Entity and Business Associate agree to modify the Contract to incorporate the terms of this Agreement and to comply with the requirements of HIPAA addressing confidentiality, security and the transmission of individually identifiable health information created, used or maintained by the Business Associate during the performance of the Contract and after Contract termination. The parties agree that any conflict between provisions of the Contract and the Agreement will be governed by the terms of the Agreement.

2. DEFINITIONS

The following terms shall have the following meaning in this Agreement. Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms specified in the Privacy Rule.

- a. “Disclosure” means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.
- b. “Incident” means a use or disclosure of PHI by the Business Associate or subcontractor not authorized by this Agreement or in writing by the Covered Entity, a complaint by an individual who is the subject of any PHI created or maintained by the Business Associate on behalf of the Covered Entity, and any Federal HIPAA related compliance contact. Also included in this definition is any attempted, successful or unsuccessful, unauthorized access, modification, or destruction of PHI, including electronic PHI, or interference with the operation of any information system that contains PHI as defined in 45 CFR 164.304.
- c. “Individual” means the person who is the subject of protected health information or the personal representative of an Individual as defined and provided for under applicable provisions of HIPAA.
- d. “Protected Health Information (PHI)” means health information, including demographic information, created, received, maintained, or transmitted in any form or media by the Business Associate, on behalf of the Covered Entity, where such information relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the payment for the provision of health care to an individual, that identifies the individual or provides a reasonable basis to believe that it can be used to identify an individual.

3. RESPONSIBILITIES OF BUSINESS ASSOCIATE

- a. **Nondisclosure.** The Business Associate shall not use or disclose any PHI except as permitted or required by the Contract or this Agreement, as permitted or required by law, or as otherwise

authorized in writing by the Covered Entity, provided that such use or disclosure would not violate the HIPAA regulations if done by the Covered Entity.

4. SAFEGUARDING AND SECURITY OF PROTECTED HEALTH INFORMATION

- a. Consistent with Attachment A, at a minimum, the Business Associate will implement, maintain, and use:
 - (i) reasonable and appropriate administrative, technical, and physical safeguards that reasonably and appropriately safeguard the confidentiality, integrity, and availability of PHI, including electronic PHI that it creates, receives, maintains, uses or transmits on behalf of the Covered Entity; and to prevent use and disclosure of PHI other than as provided for by this Agreement.
- b. The Business Associate will document PHI safeguards and security measures and agrees to provide the Covered Entity with access and review of this documentation if requested by the Covered Entity or an agent of the Covered Entity. Security measures employed by the Business Associate must be sufficient to ensure that the Covered Entity is compliant with the HIPAA privacy and security requirements for those covered services, activities, or functions performed on behalf of the Covered Entity on or before the compliance date for such requirements.
- c. **Security.** Business Associate will take any and all steps necessary to ensure the continuous security of all computerized data systems containing PHI, and provide data security procedures for the use of the Covered Entity at the end of the contract period. The steps at a minimum, shall include:
 - (i) Complying with all of the data system security provisions listed in the Attachment A of this Agreement.
 - (ii) Achieving and maintaining compliance with the HIPAA Security Rule (45 CFR Parts 160 and 164), as necessary in conducting operations on behalf of the Covered Entity under this Agreement.
 - (iii) Business Associate shall designate a Security Officer to oversee its data security program who shall be responsible for carrying out the requirements of this section and for communicating security matters with the Covered Entity.

5. REPORTING OF INCIDENTS TO COVERED ENTITY BY BUSINESS ASSOCIATE

The Business Associate agrees to inform the Covered Entity of any Incident covered by this , including an Incident reported to Business Associate by subcontractors or agents.

- a. **Discovery of Breach.** The Business Associate must inform the Covered Entity by telephone call plus email or fax immediately within the same day of the discovery of any Incident, including but not limited to the discovery of breach of security of PHI in computerized form if the PHI was, or is reasonably believed to be acquired by an unauthorized person, the discovery of any suspected security incident, intrusion or unauthorized use or disclosure of PHI in violation of this Agreement, or potential loss of confidential data affecting this agreement. Notification shall be provided to the DHS Program Contract Manager, the DHS Privacy Officer and the DHS Security Officer. If the incident occurs after business hours or on a weekend or holiday and does not involve electronic PHI, notification shall occur within the first business day that follows discovery of the incident.
- b. **Mitigation.** The Business Associate agrees to mitigate, to the extent practicable, any harmful effect known to the Business Associate created by the Incident.
- c. **Investigation of Breach.** The Business Associate shall immediately investigate the Incident.. Within one business day of the discovery, the Business Associate shall notify the Covered Entity's Program Contract Manager, the Covered Entity's Privacy Officer, and the Covered Entity's Security Officer of the following information:
 - (i) Detail of what data elements were involved and the extent of data involved in the breach,
 - (ii) A description of unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or confidential data,

- (iii) A description of where the PHI or confidential data is believed to have been improperly transmitted, sent, or utilized,
 - (iv) A description of probable causes of the improper use or disclosure.
- d. **Written Report.** The Covered Entity, at its discretion, may require a written report. If a written report is requested by the Covered Entity, the Business Associate agrees to forward a written report to the Covered Entity not more than 15 business days after such request is made. Written and verbal reports of Incidents will include a complete description of the circumstances of the Incident:
- (i) The name of persons assigned to review and investigate the Incident;
 - (ii) A description of all PHI used or disclosed during the Incident,
 - (iii) The name of persons and organizations involved in the Incident,
 - (iv) The actions the Business Associate has undertaken or will undertake to mitigate any harmful effect of the incident; and,
 - (v) A corrective action plan that includes steps the Business Associate has taken or will take to prevent future similar Incidents from occurring.
- e. **Notification to Individuals.** The Business Associate will be responsible for notifying Individuals of the Incident when the Covered Entity requires notification and to pay any cost of such notifications, as well as any costs associated with the breach, including but not limited to credit monitoring. The Business Associate must get the Covered Entity’s approval of the time, manner and content of any such notifications.
- f. **Covered Entity Contact Information.** To direct communications to above referenced Covered Entity’s staff, the Business Associate shall initiate contact as indicated herein. The Covered Entity reserves the right to make changes to the contact information by giving written notice to the Business Associate.

Covered Entity Program Manager – <complete>	DHS Privacy Officer c/o Office of Legal Counsel Department of Health Services Room 651 1 W. Wilson St. Madison, WI 53707 608-266-5484	DHS Security Officer Department of Health Services Room B150 1 W. Wilson St. Madison, WI 53707 608-261-8310
---	---	--

6. STATUTORY DUTY OF COVERED ENTITY TO REPORT MATERIAL BREACHES BY BUSINESS ASSOCIATE TO SECRETARY OF HEALTH AND HUMAN SERVICES (HHS)

Business Associate and Covered Entity agree that if the Business Associate engages in a pattern of activity or practice that constitutes a material breach or violation of this Agreement, and the Covered Entity becomes aware of such pattern or practice, the Covered Entity is required to take reasonable steps to cure the breach or end the violation, as applicable, and, if such steps are not successful and termination of the Contract is not feasible, the Covered Entity is required to report the problem to the Secretary of HHS.

7. USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION BY SUBCONTRACTORS AND AGENTS OF THE BUSINESS ASSOCIATE

The Business Associate agrees to ensure that any agents or subcontractors, to whom the Business Associate provides PHI received from, or created or received by the Business Associate on behalf of the Covered Entity, agrees to the same restrictions and conditions applicable to the Business Associate in this Agreement.

8. ACCESS TO PROTECTED HEALTH INFORMATION

At the direction of the Covered Entity, Business Associate agrees to provide access in accordance to 45 CFR 164.524 to any PHI held by the Business Associate, which Covered Entity has determined to be part of Covered Entity’s Designated Record Set, in the time and manner designated by the Covered Entity. This

access will be provided to Covered Entity or, as directed by Covered Entity, to an Individual, in order to meet requirements under the Privacy Rule.

9. AMENDMENT OR CORRECTION TO PROTECTED HEALTH INFORMATION

At the direction of the Covered Entity, the Business Associate agrees to amend or correct PHI held by the Business Associate in accordance with 45 CFR 164.526.

10. DOCUMENTATION OF DISCLOSURES OF PROTECTED HEALTH INFORMATION BY THE BUSINESS ASSOCIATE

The Business Associate agrees to document and make available to the Covered Entity or (at the direction of the Covered Entity) to an Individual such disclosures of PHI to respond to a proper request by the Individual for an accounting of disclosures of PHI, in accordance with 45 CFR 164.528.

11. INTERNAL PRACTICES

The Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of PHI available to the Covered Entity, or to the Secretary of Health and Human Services (HHS) in a time and manner determined by the Covered Entity or the Secretary or designee, for purposes of determining compliance by the Covered Entity with the requirements of HIPAA. Further, the Business Associate agrees to promptly notify the Covered Entity of communications with HHS regarding PHI and will provide the Covered Entity with copies of any PHI or other information the Business Associate has made available to HHS under this provision.

12. TERM AND TERMINATION OF AGREEMENT

- a. The Business Associate agrees that if in good faith the Covered Entity determines that the Business Associate has materially breached any of its obligations under this Agreement, the Covered Entity shall:
 - (i) Provide an opportunity for the Business Associate to cure the breach or end the violation and terminate this Agreement if the Business Associate does not cure the breach or end the violation within the time specified by the Covered Entity.
 - (ii) Immediately terminate this Agreement if the Business Associate has breached a material term of this Agreement and cure is not possible; or
 - (iii) If neither cure nor termination is feasible, report the violation to the Secretary of the U.S. Department of Health and Human Services.
- b. Before exercising either (ii) or (iii), the Covered Entity will provide written notice of preliminary determination to the Business Associate describing the violation and the action the Covered Entity intends to take.

13. RETURN OR DESTRUCTION OF PROTECTED HEALTH INFORMATION

Upon termination, cancellation, expiration or other conclusion of this Agreement, the Business Associate will:

- a. Return to the Covered Entity or, if return is not feasible, destroy all PHI and any compilation of PHI in any media or form. The Business Associate agrees to ensure that this provision also applies to PHI of the Covered Entity in possession of subcontractors and agents of the Business Associate.. The Business Associate agrees that any original record or copy of PHI in any media is included in and covered by this provision, as are all original or copies of PHI provided to subcontractors or agents of the Business Associate. The Business Associate agrees to complete the return or destruction as promptly as possible, but not more than **thirty (30)** business days after the conclusion of this Agreement. The Business Associate will provide written documentation evidencing that return or destruction of all PHI has been completed.

- b. If the Business Associate believes that the return or destruction of PHI is not feasible, the Business Associate shall provide written notification of the conditions that make return or destruction not feasible. If the Business Associate and Covered Entity agree that return or destruction of PHI is not feasible, the Business Associate shall extend the protections of this Agreement to PHI and prohibit further uses or disclosures of the PHI of the Covered Entity without the express written authorization of the Covered Entity. Subsequent use or disclosure of any PHI subject to this provision will be limited to the use or disclosure that makes return or destruction not feasible.

14. MISCELLANEOUS PROVISIONS

- a. Automatic Amendment: This Agreement shall automatically incorporate any change or modification to HIPAA as of the effective date of the change or modification. The Business Associate agrees to maintain compliance with all changes or modifications to HIPAA as required.
- b. Interpretation of Terms or Conditions of Agreement: Any ambiguity in this Agreement shall be construed and resolved in favor of a meaning that permits the Covered Entity and Business Associate to comply with HIPAA.

IN WITNESS WHEREOF, the undersigned have caused this Agreement to be duly executed by their respective representatives.

COVERED ENTITY

BUSINESS ASSOCIATE

By: _____

By: _____

Title: _____

Title: _____

Date: _____

Date: _____

Wisconsin Department of Health Services – Attachment A

1. Confidentiality Statement. All persons that will be working with the Covered Entity's PHI must sign a confidentiality statement supplied by the Business Associate. This statement must be signed by the workforce member prior to access to DHS PHI. The statement must be renewed annually.
2. Background Check. Before a member of the Business Associate's workforce may access PHI, Business Associate must conduct a thorough background check of that individual and evaluate results to assure there is no indication that the individual may present a risk for theft of confidential data.
3. Laptop Encryption. All laptops that process and/or store PHI must be encrypted with Covered Entity's approved solution. All laptops that process and/or store PHI must be encrypted with Covered Entity's approved solution when available. An encryption solution from the Federal Governments blanket purchase agreements (BPA) to protect sensitive, unclassified data is acceptable. The encryption solution must be full-disk.
4. Minimum Necessary. Only the minimum amount of PHI may be downloaded to a laptop or hard drive when absolutely necessary for business purposes.
5. Removable Media Devices. All electronic files that contain the Covered Entity's PHI must be encrypted when stored on any removable media type device (i.e., USB flash drive, floppies, CD/DVD/etc.).
6. Email Security. All emails including the Covered Entity's PHI must be sent in an encrypted method.
7. Antivirus Software. All workstations, laptops and other systems that process and/or store the Covered Entity's PHI must have a commercial third-party anti-virus software solution with a minimum daily automatic update.
8. Patch Management. All workstations, laptops and other systems that process and/or store the Covered Entity's PHI must have security patches applied and be up-to-date.
9. User ID's and Password Controls. All users must be issued a unique user name for accessing the Covered Entity's PHI. Passwords are not to be shared. They must be at least six to eight characters or more, minimum of two alpha and one numeric characters, use of special characters if allowed and use upper/lower case where allowed. They must be changed every 60 days.
10. Data Destruction. If the Business Associate must dispose of the Covered Entity's data, it must be destroyed using U.S. Department of Defense standard methods for data destruction
11. Remote Access. Any remote access to the Covered Entity's PHI must be executed over an encrypted method approved by the Covered Entity. All remote access must be limited to minimum necessary and least privilege principles.
12. Paper Document Controls. Supervision of data. Business Associate must have a policy that:
 - a. The Covered Entity's PHI in paper form shall not be left unattended at any time, unless it is locked in a file, cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information.
 - b. The Covered Entity's PHI in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial planes.
 - c. Confidential Destruction. The Covered Entity's PHI must be disposed of through confidential means such as shredding and pulverizing.

- d. Removal of Data. The Covered Entity's PHI must not be removed from the premises of the Business Associate except for routine business purposes or with the express written permission of the Covered Entity.

- e. Faxing. Faxes containing the Covered Entity's PHI shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending.

- f. Mailing. The Covered Entity's PHI shall only be mailed using secure methods. Electronic media such as disks and other transportable media sent through the mail must be encrypted.