Attachment B
NORTH DAKOTA DEPARTMENT OF HUMAN SERVICES
Business Associate Agreement

This Business Associate Agreement is entered into by and between the North Dakota Department of Human Services and [Insert Name of Business Associate] each individually a "Party" and collectively the "Parties." This Agreement is hereby incorporated into the underlying contract {insert contract title/name} between the parties dated {insert date of original contract}.

1. DEFINITIONS

Terms used, but not otherwise defined, in this Agreement have the same meaning as those terms in the HIPAA Rules.

Catch-all definitions:

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, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

a. Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR § 160.103, and in reference to the party to this Agreement, shall mean [Insert Name of Business Associate].

b. Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR § 160.103, and in reference to the party to this Agreement, shall mean the North Dakota Department of Human Services.

c. Electronic Protected Health Information. "Electronic Protected Health Information" (ePHI) shall generally have the same meaning as the term "electronic protected health information" at 45 CFR § 160.103.

d. HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

e. Protected Health Information. "Protected Health Information" (PHI) shall generally have the same meaning as the term "protected health information" at 45 CFR § 160.103 that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity.

2. OBLIGATIONS OF BUSINESS ASSOCIATE

a. Business Associate shall not use or disclose PHI except as permitted or required by this Agreement, as required by law, or as otherwise authorized in writing by Covered Entity.

b. Business Associate shall not use or disclose PHI in a manner that would violate Subpart E of 45 CFR § 164 if done by Covered Entity, except that Business Associate may use

PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of Business Associate.

c. 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 in accordance with 45 CFR § 164.502(b).

d. Business Associate shall not share, use, or disclose PHI in any form via any medium with any third party beyond the boundaries and jurisdiction of the United States of America without express written authorization from Covered Entity.

e. Business Associate shall ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate agree to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such PHI, in accordance with 45 CFR § 164.502(e)(1) and § 164.308(b).

f. Business Associate shall use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to ePHI, to prevent use or disclosure of PHI other than as provided for by this Agreement.

g. Business Associate shall within ten (10) business days of receiving written notice from Covered Entity, provide access to any PHI in a Designated Record Set, in the manner designated by the Covered Entity, as necessary to satisfy Covered Entity's obligations under 45 CFR § 164.524.

h. Business Associate shall within twenty (20) business days of receiving written notice from Covered Entity, make any amendments to PHI in a Designated Record Set, as directed or agreed to by Covered Entity pursuant to 45 CFR § 164.526, or take other measures as necessary to satisfy the Covered Entity's obligations under 45 CFR § 164.526.

i. Business Associate shall document and maintain the PHI required to provide for an accounting of disclosures of PHI to Covered Entity as necessary to satisfy Covered Entity's obligations under 45 CFR § 164.528.

j. Business Associate shall within twenty (20) business days of receiving written notice from Covered Entity, make available to Covered Entity, or (at the direction of Covered Entity) to an Individual, such disclosures of PHI required to respond to a request for an accounting of disclosures in accordance with 45 CFR § 164.528.

k. Business Associate shall make its internal practices, books, and records available to the Secretary and to Covered Entity for purpose of determining compliance with the HIPAA Rules.

3. REPORTING OF A VIOLATION TO COVERED ENTITY BY BUSINESS ASSOCIATE

Business Associate shall report to Covered Entity's Breach Investigation Team (BIT) via email at dhsbreach@nd.gov, any use or disclosure of PHI not provided for by this Agreement, of which it becomes aware, including breaches of unsecured PHI as required at 45 CFR § 164.410, and any Security Incident of which it becomes aware, immediately, and in no case later than ten (10) business days after the use or disclosure.

a. Security Incident. "Security Incident" means (as defined by 45 CFR § 164.304), the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. For purposes of clarification of this Section, Security Incident includes use, disclosure, modification, or destruction of PHI by an employee or otherwise authorized user of its system of which Business Associate becomes aware. Business Associate shall track all Security Incidents and shall report such Security Incidents in summary fashion as may be requested by the Covered Entity.

   i. Unsuccessful Security Incidents. Business Associate and Covered Entity agree that this Agreement constitutes notice from Business Associate of such Unsuccessful Security Incidents. By way of example, Covered Entity and Business Associate consider the following to be illustrative of Unsuccessful Security Incidents when they do not result in unauthorized access, use, disclosure, modification, or destruction of PHI or interference with an information system:

      1. Pings on Business Associate's firewall;

      2. Port Scans, which are attempts to log on to a system or enter a database with an invalid password or username;

      3. Denial-of-service attacks that do not result in a server being taken off-line; and

      4. Malware (e.g., worms, viruses).

b. Discovery of a Violation. If the use or disclosure amounts to a breach of unsecured PHI, Business Associate shall ensure its report is made to Covered Entity's Breach Investigation Team (BIT) via email at dhsbreach@nd.gov immediately upon becoming aware of the Breach, and in no case later than ten (10) business days after discovery. The Violation shall be treated as "discovered" on the first day which the Violation is known to the Business Associate or, by exercising reasonable diligence would have been known to the Business Associate. For purposes of clarification of this Section, Business Associate must notify Covered Entity of an incident involving the acquisition, access, use, or disclosure of PHI in a manner not permitted under 45 CFR Part E within ten (10) business days after an incident even if Business Associate has not conclusively determined within that time that the incident constitutes a Breach as defined by HIPAA.

c. Investigation of Breach. Business Associate shall immediately investigate the Violation and report in writing within ten (10) business days to Covered Entity with the following information:

   i. Each Individual whose PHI has been or is reasonably believed to have been accessed, acquired, or disclosed during the Incident;

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

   iii. A description of unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or confidential data;

iv. A description of where the PHI or confidential data is believed to have been improperly transmitted, sent, or utilized;

v. A description of probable causes of the improper use or disclosure;

vi. A brief description of what Business Associate is doing to investigate the Incident, to mitigate losses, and to protect against further Violations;

vii. The actions Business Associate has undertaken or will undertake to mitigate any harmful effect of the occurrence; and

viii. A Corrective Action Plan that includes the steps Business Associate has taken or shall take to prevent future similar Violations.

d. Breach Notification.

i. Business Associate shall cooperate and coordinate with Covered Entity in the preparation of any reports or notices to the Individual, required to be made under the HIPAA Rules or any other Federal or State laws, rules or regulations, provided that any such reports or notices shall be subject to the prior written approval of Covered Entity.

ii. Covered Entity shall make the final determination whether the Breach requires notices to affected Individuals and whether the notices shall be made by Covered Entity or Business Associate.

iii. For any notice regarding a Breach of unsecured PHI caused by Business Associate that Covered Entity is required to provide pursuant to 45 CFR §§ 164.404 – 164.408, Business Associate shall reimburse Covered Entity for all costs associated with Covered Entity's obligation of notifying affected Individuals, the Secretary, and the media.

e. Mitigation. Business Associate shall mitigate to the extent practicable, any harmful effects known to the Business Associate of a use, disclosure, or loss of PHI by Business Associate in violation of the requirements of this Agreement, including, without limitation, any Security Incident or Breach of unsecure PHI. Business Associate shall reasonably cooperate with the Covered Entity'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.

4. TERM AND TERMINATION OF AGREEMENT

a. Term. The Term of this Agreement becomes effective when the last Party signs and dates this Agreement, and terminates when all of the PHI provided by Covered Entity, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or if it is infeasible to return or destroy PHI, protections are extended to the PHI, in accordance with the termination provisions in this Section and in compliance with federal law.

b. Automatic Termination. This Agreement automatically terminates upon the termination or expiration of the services provided.

c. Termination for Cause. Business Associate agrees that if in good faith Covered Entity determines that Business Associate has materially breached any of its obligations under this Agreement, Covered Entity may:

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

   ii. Require Business Associate to cure the breach or end the violation within thirty (30) business days;

   iii. Terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

   iv. Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or

d. Report Business Associate's violation to the Secretary if neither termination nor cure is feasible.

e. Before exercising either (c)(ii) or (c)(iii), Covered Entity shall provide written notice of preliminary determination to Business Associate describing the violation and the action Covered Entity intends to take.

5. RETURN OR DESTRUCTION OF PROTECTED HEALTH INFORMATION

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

a. Return to Covered Entity or, if return is not feasible, destroy all PHI and any compilation of PHI in any media or form. Business Associate agrees to ensure that this provision also applies to PHI in possession of subcontractors and agents of Business Associate. Business Associate agrees that any original record or copy of PHI in any media is included in and covered by this provision, as well as all originals or copies of PHI provided to subcontractors or agents of Business Associate. 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. Business Associate will provide written documentation evidencing that return or destruction of all PHI has been completed.

b. If Business Associate 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 the Secretary. Acceptable methods for destroying PHI include:

   i. For paper, film, or other hard copy media: shredding or destroying in order that PHI cannot be read or reconstructed; and

ii. For electronic media: clearing, purging, or destroying consistent with the standards of the National Institute of Standards and Technology (NIST).

Redaction is specifically excluded as a method of destruction of PHI.

c. If Business Associate believes that the return or destruction of PHI is not feasible, Business Associate shall provide written notification of the conditions that make return or destruction not feasible. If Business Associate determines that return or destruction of PHI is not feasible, Business Associate shall extend the protections of this Agreement to the PHI and prohibit further uses or disclosures of the PHI without the express written authorization of 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.

6. OBLIGATIONS OF COVERED ENTITY

a. Notice of Privacy Practices. Covered Entity shall notify Business Associate of any limitation in its Notice of Privacy Practices to the extent such limitations affect Business Associate's permitted uses or disclosures of PHI.

b. Notice of Changes in Permission. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes affect Business Associate's permitted uses or disclosures of PHI.

c. Notice of Restrictions. Covered Entity shall notify Business Associate of any restrictions of the use or disclosure of PHI to which Covered Entity has agreed, to the extent that such restrictions affect Business Associate's permitted use or disclosure of PHI.

d. Permissible Requests. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA Rules if used or disclosed by Covered Entity.

7. MISCELLANEOUS PROVISIONS

a. Regulatory Reference. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

b. Amendment. The Parties agree to take such action to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the HIPAA Rules. Business Associate and Covered Entity shall comply with any amendment to the HIPAA Rules, and related regulations upon the effective date of such amendment, regardless of whether this Agreement has been formally amended.

c. Survival. The respective rights and obligations of Business Associate under Section 2 of this Agreement shall survive the termination or expiration of this Agreement.

d. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity and Business Associate to comply with the HIPAA Rules.

e. Headings. Paragraph Headings used in this Agreement are for the convenience of the Parties and shall have no legal meaning in the interpretation of this Agreement.

f. Severability. With respect to any provision of this Agreement finally determined by a court of competent jurisdiction to be unenforceable, such court shall have jurisdiction to reform such provision so that it is enforceable to the maximum extent permitted by applicable law, and the Parties shall abide by such court's determination. In the event that any provision of this Agreement cannot be reformed, such provision shall be deemed to be severed from this Agreement, but every other provision of this Agreement shall remain in full force and effect.

g. No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer upon any person other than the Parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

h. Applicable Law and Venue. This Business Associate Agreement is governed by and construed in accordance with the laws of the State of North Dakota. Any action commenced to enforce this Agreement must be brought in the District Court of Burleigh County, North Dakota.

i. Contact Persons. Business Associate shall identify "key contact persons" in Attachment "A" for all matters relating to this Agreement and shall notify Covered Entity of any change in these key contacts during the term of this Agreement in writing within ten (10) business days.

8. ENTIRE AGREEMENT

This Agreement contains all of the agreements and understandings between the Parties with respect to the subject matter of this Agreement. No agreement or other understanding in any way modifying the terms of this Agreement will be binding unless made in writing as a modification or amendment to this Agreement and executed by both Parties.

IN WITNESS OF THIS, North Dakota Department of Human Services ("Covered Entity") and {insert Business Associate} ("Business Associate") agree to and intend to be legally bound by all terms and conditions set forth above and hereby execute this Agreement as of the effective date set forth above.

For Covered Entity:	For Business Associate
(Signature):_____	(Signature):_____
(Print Name):_____	(Print Name):_____
(Title):_____	(Title):_____
(Date):_____	(Date):_____

ATTACHMENT "B"
BUSINESS ASSOCIATE KEY CONTACT PERSONS

When applicable, Business Associate shall notify Covered Entity of any change in key contacts during the term of this Agreement in writing within ten business days.

Website URL (if applicable):	

FIRST POINT OF CONTACT	
Name:	
Title:	
Address:	
Phone Number:	
Fax Number:	
Email Address:	

SECOND POINT OF CONTACT	
Name:	
Title:	
Address:	
Phone Number:	
Fax Number:	
Email Address:	

Business Associate

(Signature):_____

(Print Name): _____

(Title):_____

(Date):_____