Business Associate Agreement

THIS ADDENDUM supplements and is made a part of the Iowa Department of Human Services ("Agency") Contract (hereinafter, the "Underlying Agreement") between the Agency and the Contractor ("the Business Associate").

1. **Purpose.**
   The Business Associate performs certain services on behalf of or for the Agency pursuant to the Underlying Agreement that require the exchange of information that is protected by the Health Insurance Portability and Accountability Act of 1996, as amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5) (the "HITECH Act") and the federal regulations published at 45 C.F.R. parts 160 and 164 (collectively "HIPAA"). The Agency is a hybrid Covered Entity as that term is defined in HIPAA. For purposes of this agreement, the portions of the Agency that fall under the purview of HIPAA shall be referred to as the "Covered Entity." The parties to the Underlying Agreement are entering into this Addendum to establish the responsibilities of both parties regarding Protected Health Information and to bring the Underlying Agreement into compliance with HIPAA.

2. **Definitions.**
   Unless otherwise provided in this Addendum, capitalized terms have the same meanings as set forth in HIPAA.

3. **Obligations of Business Associate.**
   a. *Security Obligations.* Sections 164.308, 164.310, 164.312 and 164.316 of title 45, Code of Federal Regulations, apply to the Business Associate in the same manner that such sections apply to the Covered Entity. The Business Associate's obligations include but are not limited to the following:
      - Implementing administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic Protected Health Information that the Business Associate creates, receives, maintains, or transmits on behalf of the Covered Entity as required by HIPAA;
      - Ensuring that any agent, including a subcontractor, to whom the Business Associate provides such information agrees to implement reasonable and appropriate safeguards to protect the data; and
      - Reporting to the Covered Entity any security incident of which it becomes aware.

   b. *Privacy Obligations.* To comply with the privacy obligations imposed by HIPAA, Business Associate agrees to:
      - Not use or further disclose information other than as permitted or required by the Underlying Agreement, this Addendum, or as required by law;
      - Abide by any Individual's request to restrict the disclosure of Protected Health Information consistent with the requirements of Section 13405(a) of the HITECH Act;
      - Use appropriate safeguards to prevent use or disclosure of Protected Health Information other than as provided for by the Underlying Agreement and this Addendum;
      - Report to the Covered Entity any use or disclosure of Protected Health Information not provided for by the Underlying Agreement of which the Business Associate becomes aware;
      - Ensure that any agents, including a subcontractor, to whom the Business Associate provides Protected Health Information received from the Covered Entity or created or received by the Business Associate on behalf of the Covered Entity agrees to the same

restrictions and conditions that apply to the Business Associate with respect to such information;

- Make available to the Covered Entity within thirty (30) days Protected Health Information to comply with an Individual's right of access to their Protected Health Information in compliance with 45 C.F.R. § 164.524 and Section 13405(f) of the HITECH Act;
- Make available to the Covered Entity within thirty (30) days Protected Health Information for amendment and incorporate any amendments to Protected Health Information in accordance with 45 C.F.R. § 164.526;
- Make available to the Covered Entity within fifteen (15) days the information required to provide an accounting of disclosures in accordance with 45 C.F.R. § 164.528 and Section 13405(c) of the HITECH Act;
- Make its internal practices, books, and records relating to the use and disclosure of Protected Health Information received from the Covered Entity, or created or received by the Business Associate on behalf of the Covered Entity, available to the Secretary for purposes of determining the Covered Entity's compliance with HIPAA;
- To the extent practicable, mitigate any harmful effects that are known to the Business Associate of a use or disclosure of Protected Health Information in violation of this Addendum;
- Use and disclose an Individual's Protected Health Information only if such use or disclosure is in compliance with each and every applicable requirement of 45 C.F.R. § 164.504(e);
- Refrain from exchanging any Protected Health Information with any entity of which the Business Associate knows of a pattern of activity or practice that constitutes a material breach or violation of HIPAA;
- To comply with Section 13405(b) of the HITECH Act when using, disclosing, or requesting Protected Health Information in relation to this Addendum by limiting disclosures as required by HIPAA;
- Refrain from receiving any remuneration in exchange for any Individual's Protected Health Information unless (1) that exchange is pursuant to a valid authorization that includes a specification of whether the Protected Health Information can be further exchanged for remuneration by the entity receiving Protected Health Information of that Individual, or (2) satisfies one of the exceptions enumerated in Section 13405(d)(2) of the HITECH Act or HIPAA regulations; and
- Refrain from marketing activities that would violate HIPAA, specifically Section 13406 of the HITECH Act.

c. *Permissive Uses.* The Business Associate may use or disclose Protected Health Information that is disclosed to it by the Covered Entity under the following circumstances:

- Business Associate may use the information for its own management and administration and to carry out the legal responsibilities of the Business Associate.
- Business Associate may disclose the information for its own management and administration and to carry the legal responsibilities of the Business Associate if (1) the disclosure is required by law, or (2) the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

d. Breach Notification. In the event that the Business Associate discovers a Breach of Unsecured Protected Health Information, the Business Associate agrees to take the following measures within 30 calendar days after the Business Associate first discovers the incident:

- To notify the Covered Entity of any Breach. Such notice by the Business Associate shall be provided without unreasonable delay, except where a law enforcement official determines that a notification would impede a criminal investigation or cause damage to national security. For purposes of this Addendum, the Business Associate is deemed to have discovered the Breach as of the first day on which such Breach is known to the Business Associate or by exercising reasonable diligence, would have been known to the Business Associate, including any person, other than the individual committing the Breach, that is a workforce member or agent of the Business Associate;
- To include to the extent possible the identification of the Individuals whose Unsecured Protected Health Information has been, or is reasonably believed to have been, the subject of a Breach;
- To complete and submit the Breach Notice form to the Covered Entity (see Exhibit A); and
- To include a draft letter for the Covered Entity to utilize to notify the Individuals that their Unsecured Protected Health Information has been, or is reasonably believed to have been, the subject of a Breach. The draft letter must include, to the extent possible:
    1. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;
    2. A description of the types of Unsecured Protected Health Information that were involved in the Breach (such as full name, Social Security Number, date of birth, home address, account number, disability code, or other types of information that were involved);
    3. Any steps the Individuals should take to protect themselves from potential harm resulting from the Breach;
    4. A brief description of what the Covered Entity and the Business Associate are doing to investigate the Breach, to mitigate harm, and to protect against any further Breaches; and
    5. Contact procedures for Individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, web site, or postal address.

4. Addendum Administration.

a. Termination. The Covered Entity may terminate this Addendum for cause if the Covered Entity determines that the Business Associate or any of its subcontractors or agents has breached a material term of this Addendum. Termination of either the Underlying Agreement or this Addendum shall constitute termination of the corresponding agreement.

b. Effect of Termination. At termination of the Underlying Agreement or this Addendum, the Business Associate shall return or destroy all Protected Health Information received or created in connection with this Underlying Agreement, if feasible. If such return or destruction is not feasible, the Business Associate will extend the protections of this Addendum to the Protected Health Information and limit any further uses or disclosures. The Business Associate will provide the Covered Entity in writing a description of why return or destruction of the information is not feasible.

c. Compliance with Confidentiality Laws. Business Associate acknowledges that it must comply with all laws that may protect the Protected Health Information received and will comply with all such laws, which include but are not limited to the following:

- *Medicaid applicants and recipients*: 42 U.S.C. § 1396a(a)(7); 42 C.F.R. §§ 431.300 - .307; Iowa Code § 217.30;
- *Mental health treatment*: Iowa Code chapters 228, 229;
- *HIV/AIDS diagnosis and treatment*: Iowa Code § 141A.9; and

- *Substance abuse treatment:* 42 U.S.C. § 290dd-3; 42 U.S.C. § 290ee-3; 42 C.F.R. part 2; Iowa Code §§ 125.37, 125.93.

d. *Indemnification for Breach Notification.* Business Associate shall indemnify the Covered Entity for costs of an action required to be taken under any law or regulation as a result of any Breach by the Business Associate or any subcontractor in a manner not permitted under 45 C.F.R. part E.

e. *Amendment.* The Covered Entity may amend the Addendum from time to time by posting an updated version of the Addendum on the Agency's website at: http://www.dhs.state.ia.us/Consumers/Health/HIPAA/Home.html, and providing the Business Associate electronic notice of the amended Addendum. The Business Associate shall be deemed to have accepted the amendment unless the Business Associate notifies the Covered Entity of its non-acceptance in accordance with the Notice provisions of the Contract within 30 days of the Covered Entity's notice referenced herein. Any agreed alteration of the then current Covered Entity Addendum shall have no force or effect until the agreed alteration is reduced to a Contract amendment and signed by the Contractor, Agency Director, and the Agency Security and Privacy Officer.

f. *Survival.* The obligations of the Business Associate shall survive this Addendum's termination.

g. *No Third Party Beneficiaries.* There are no third party beneficiaries to this agreement between the parties. The Underlying Agreement and this Addendum are intended to only benefit the parties to the agreement.

h. *Effective Date*. This Addendum is effective as of the Underlying Agreement's Effective Date.

EXHIBIT A: NOTIFICATION TO THE COVERED ENTITY OF BREACH OF UNSECURED PROTECTED HEALTH INFORMATION

NOTE: The Business Associate must use this form to notify the Covered Entity of any Breach of Unsecured Protected Health Information. Immediately provide a copy of this completed form to (1) the Contract Manager, in compliance with the Notice Requirements of the Underlying Agreement, and (2) the Agency Security and Privacy Officer at:

Iowa Department of Human Services
Attn: Security & Privacy Officer
1305 E. Walnut, 1st Floor, DDM
Des Moines, IA 50319

Contract Information	
Contract Number	**Contract Title**
Contractor Contact Information	
Contact Person for this Incident:	
Contact Person's Title:	
Contact's Address:	
Contact's E-mail:	
Contact's Telephone No.:	

Business Associate hereby notifies the Covered Entity that there has been a Breach of Unsecured (unencrypted) Protected Health Information that Business Associate has used or has had access to under the terms of the Business Associate Agreement, as described in detail below:

Breach Details	
Date of Breach	**Date of Discovery of Breach**
Detailed Description of the Breach	
Types of Unsecured Protected Health Information involved in the Breach (such as full name, SSN, Date of Birth, Address, Account Number, Disability Code, etc).	
What steps are being taken to investigate the breach, mitigate losses, and protect against any further breaches?	
Number of Individuals Impacted	**If over 500, do individuals live in multiple states?**
	YES | NO

Signature:_____ **Date:** _____