Business Associate Agreement

To the extent that this Business Associate Agreement is incorporated into the Contract by reference, the Vendor acts as the Business Associate of the agency or agencies designated in Attachment A to this Business Associate Agreement as Covered Entities under the Health Insurance Portability and Accountability Act of 1996, as amended, and the federal regulations published at 45 CFR part 160 and 164.

For purposes of this Business Associate Agreement, the Vendor (the "Business Associate") agrees to comply with this Business Associate Agreement (BAA). This Business Associate Agreement ("BAA") supplements and is made a part of the Contract (hereinafter, the "Underlying Agreement") between the Covered Entities and the Business Associate.

1. Purpose.

The Business Associate performs certain services on behalf of or for the Agency pursuant to the Underlying Agreement that may include the exchange of information that is protected by the Health Insurance Portability and Accountability Act of 1996, as amended, and the HIPAA Rules (collectively "HIPAA"). The parties to the Underlying Agreement are entering into this BAA to establish the responsibilities of both parties regarding Protected Health Information and to bring the Underlying Agreement into compliance with HIPAA.

2. Definitions.

The following terms used in this BAA shall have the same meaning as those terms in the HIPAA Rules: Breach, Designated Record Set, Disclosure, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, 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 C.F.R. § 160.103, and in reference to the party to this BAA, shall mean the Vendor.

b. *Covered Entity.* "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 C.F.R. § 160.103. For the Iowa Veterans Home, in reference to the party to this BAA shall mean the Agency. For the Department of Human Services, in reference to the party to this BAA shall mean the portions of the Agency which is a "hybrid" entity under HIPAA that fall under the purview of HIPAA.

c. *HIPAA Rules.* "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164.

3. Obligations and Activities of Business Associate.

The Business Associate agrees to:

a. Not Use or Disclose Protected Health Information other than as permitted or required by this BAA or as Required By Law;

b. Use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to Protected Health Information, to prevent Use or Disclosure of Protected Health Information other than as provided for by this BAA;

c. Report to the Covered Entity any Use or Disclosure of Protected Health Information not provided for by this BAA of which it becomes aware, including Breaches of Unsecured Protected Health Information as required at 45 C.F.R. § 164.410, and any Security Incident of which it becomes aware in accordance with subsection 7, below;

d. In accordance with 45 C.F.R. § 164.502(e)(1)(ii) and 45 C.F.R. § 164.308(b)(2), if applicable, ensure that any Subcontractors that create, receive, maintain, or transmit Protected Health

Information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information;

e. Make available Protected Health Information in a Designated Record Set to the Covered Entity as necessary to satisfy the Covered Entity's obligations under 45 C.F.R. §164.524;

f. Make any amendment(s) to Protected Health Information in a Designated Record Set as directed or agreed to by the Covered Entity pursuant to 45 C.F.R. §164.526, or take other measures as necessary to satisfy the Covered Entity's obligations under 45 C.F.R. § 164.526;

g. Maintain and promptly make available, as directed by the Covered Entity, the information required to provide an accounting of Disclosures to the Covered Entity as necessary to satisfy the Cover Entity's obligations under 45 C.F.R. § 164.528;

h. Within 5 business days forward any request that the Business Associate receives directly from an Individual who (1) seeks access to Protected Health Information held by the Business Associate pursuant to this BAA, (2) requests amendment of Protected Health Information held by the Business Associate pursuant to this BAA, or (3) requests an accounting of Disclosures, so that the Covered Entity can coordinate the response;

i. To the extent the Business Associate is to carry out one or more of the Covered Entity's obligation(s) under Subpart E of 45 C.F.R. Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s); and

j. Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

4. Permitted Uses and Disclosures by the Business Associate.

a. The Business Associate may Use or Disclose Protected Health Information received in relation to the Underlying Agreement as necessary to perform the services set forth in the Underlying Agreement.

b. The Business Associate may use or disclose Protected Health Information as is required by law.

c. The Business Associate is not authorized to de-identify Protected Health Information in accordance with 45 C.F.R. § 164.514(a)-(c) unless expressly authorized to do so in writing by the Covered Entity's Security and Privacy Officer.

d. The Business Associate agrees to make Uses and Disclosures and Requests for Protected Health Information consistent with the Covered Entity's Minimum Necessary policies and procedures.

e. The Business Associate may not Use or Disclose Protected Health Information in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by the Covered Entity.

f. The Business Associate may Use or Disclose the Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided the Disclosures are Required By Law, or the Business Associate obtains reasonable assurances from the person to who the information is Disclosed that the information will remain confidential and used or further Disclosed only as Required By Law or for the purposes 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 Protected Health Information has been Breached.

5. Obligations of the Covered Entity.

a. The Covered Entity will notify the Business Associate of any limitation(s) in the Notice of Privacy Practices of Covered Entity under 45 C.F.R. § 164.520, to the extent that such Limitation may affect the Business Associate's Use or Disclosure of Protected Health Information.

b. The Covered Entity will notify the Business Associate of any changes in, or revocation of, the permission by an Individual to Use or Disclose his or her Protected Health Information, to the extent that such changes may affect the Business Associate's Use or Disclosure of Protected

Health Information.

c. The Covered Entity shall notify the Business Associate of any restriction on the Use or Disclosure of Protected Health Information that the Covered Entity has agreed to or is required to abide by under 45 C.F.R. § 164.522, to the extent that such restriction may affect the Business Associate's Use or Disclosure of Protected Health Information.

6. Permissible Requests by the Covered Entity.

The Covered Entity shall not request the Business Associate to Use or Disclose Protected Health Information in any manner that would not be permissible under Subpart E of 45 C.F.R. Part 164 if done by the Covered Entity.

7. Breach Notification Obligations of the Business Associate.

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 5 business days after the Business Associate first discovers the incident:

a. 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 BAA, 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;

b. 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;

c. To complete and submit the Information Security Data Breach Incident Report form located on the Agency's website as set forth in Exhibit A.

d. To draft and provide written notification to 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:

i. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

ii. 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);

iii. Any steps the Individuals should take to protect themselves from potential harm resulting from the Breach;

iv. 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

v. Contact procedures for Individuals to ask questions or learn additional information, which shall include Covered Entity contact information, including a toll-free telephone number, an e-mail address, web site, or postal address.

8. Administration

a. Term and Termination. This BAA is effective on the date of its incorporation into the Underlying Agreement. The Covered Entity may terminate this BAA 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 BAA. The Covered Entity will provide written notice to the

Business Associate requesting that the Business Associate remedy the breach within the time frame provided in the notice. The remedy time frame provided the Business Associate will be consistent with the severity of the breach. The Covered Entity reserves the right to terminate the BAA without notice in the event that the Covered Entity determines, in its sole discretion, that notice is either infeasible or inappropriate under the circumstances. Expiration or termination of either the Underlying Agreement or this BAA shall constitute expiration or termination of the corresponding agreement.

b. *Obligation to Return PHI, Destroy PHI, or Extend Protections to Retained PHI.* Upon expiration or termination of this BAA for any reason, the Business Associate shall return to the Covered Entity or destroy all Protected Health Information received from Covered Entity, or created, maintained, or received by the Business Associate on behalf of the Covered Entity, that the Business Associate still maintains in any form. Return or destruction of Protected Health Information shall take place in accordance with the requirements for such return or destruction as set forth in the Underlying Agreement or as otherwise directed by the Covered Entity. The Business Associate shall retain no copies of the Protected Health Information unless such return or destruction is not feasible. If return or destruction of the Protected Health Information is not feasible, upon expiration or termination of this BAA, the Business Associate shall:

i. Retain only that Protected Health Information that is necessary for the Business Associate to continue its proper management and administration or to carry out its legal responsibilities to the extent Required By Law;
ii. Return to the Covered Entity or destroy the remaining Protected Health Information that the Business Associate still maintains in any form;
iii. Continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to Protected Health Information to prevent Use or Disclosure of the Protected Health Information, other than as provided for in this Section, for as long as the Business Associate retains the Protected Health Information;
iv. Not Use or Disclose the Protected Health Information retained by the Business Associate other than for the purposes for which such Protected Health Information was retained and subject to the same conditions set out in subsection 4(e) above under "Permitted Uses and Disclosures by the Business Associate" which applied prior to termination; and
v. Return to the Covered Entity or destroy the Protected Health Information retained by the Business Associate when it is no longer needed by the Business Associate for its proper management and administration or to carry out its legal responsibilities.

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

i. Medicaid applicants and recipients: 42 U.S.C. § 1396a(a)(7); 42 C.F.R. §§ 431.300 - .307; Iowa Code § 217.30;
ii. Mental health treatment: Iowa Code chapters 228, 229;
iii. HIV/AIDS diagnosis and treatment: Iowa Code § 141A.9; and
iv. Substance abuse treatment: 42 U.S.C. § 290dd-2; 42 C.F.R. part 2; Iowa Code §§ 125.37, 125.93.
v. Consumer personal information: Iowa Code ch. 715C.

d. *Financial Obligations for Breach Notification.*

i. To the extent that the Business Associate is a governmental agency subject to the provisions of Iowa Code § 679A.19, any dispute between the Business Associate and the Agency, including but not limited to the incursion of any costs, liabilities,

damages, or penalties related to the Business Associate's breach of this BAA, shall be submitted to a board of arbitration in accordance with Iowa Code § 679A.19.

ii. To the extent that the Business Associate is not subject to the provisions of Iowa Code § 679A.19, the Business Associate shall defend, indemnify, and hold harmless the Covered Entity from costs, liabilities, damages, or penalties incurred as a result of the Business Associate or any Subcontractor's breach of this BAA, the Underlying Agreement, or conduct of the Business Associate or the Business Associate's Subcontractor not in compliance with 45 C.F.R. Part 164, subpart E. Such liability shall not attach to disclosures made at the express written direction of the Covered Entity.

iii. The Business Associate's obligations under this subsection 8(d) are not limited to third-party claims but shall also apply to claims by the Covered Entity against the Business Associate.

e. *Amendment.* The Covered Entity may amend the BAA from time to time by posting an updated version of the BAA on the Agency's website at: https://ocio.iowa.gov/information-technology-procurement and providing the Business Associate electronic notice of the amended BAA. 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 not part of the then current Covered Entity BAA shall have no force or effect until the agreed alteration is reduced to a Contract amendment and signed by the Business Associate, Agency Director and the Covered Entity or Entities Security and Privacy Officer(s).

f. *Survival.* All obligations of the Agency and the Business Associate incurred or existing under this BAA as of the date of expiration or termination will survive the expiration or termination of this BAA.

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

h. *Miscellaneous.*

i. *Regulatory References.* A reference in this BAA to a section in the HIPAA Rules means the section as it may be amended from time to time.

ii. *Interpretation.* Any ambiguity in this BAA shall be interpreted to permit compliance with the HIPAA Rules.

iii. *Applicable Law.* Except to the extent preempted by federal law, this BAA shall be governed by and construed in accordance with the same internal laws as that of the Underlying Agreement.

iv. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirement of the HIPAA Rules and any other applicable law.

[VENDOR] (Business Associate)	Iowa Veterans Home (Agency)
By: _____	By: _____
Signature: _____	Signature: _____
Title: _____	Title: _____
Date: _____	Date: _____

Attachment A

COVERED ENTITIES AND CORRESPONDING INFORMATION

Name of Covered Entity	**Information Security Data Breach Incident Report for URL**	**Address**	**Contact Information**
Iowa Department of Human Services	http://www.dhs.state.ia.us/Consumers/Health/HIPAA/Home.html;	DHS Security and Privacy Office Iowa Department of Human Services 1305 E Walnut Street, 1st Floor Des Moines, IA 50319-0114	Phone: 1-800-803-6591 e-mail: hipaa@dhs.state.ia.us
Iowa Veterans Home	http://www.dhs.state.ia.us/Consumers/Health/HIPAA/Home.html		