Business Associate Agreement

I. Definitions

Catch-all definition:

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, 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 CFR 160.103, and in reference to the party to this agreement, shall mean _____.

(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 State of Arkansas, Department of Finance and Administration, Employee Benefits Division.**

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

II. Obligations and Activities of Business Associate

Business Associate agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware; Business Associate shall notify Covered Entity by the end of the next business day of the Business Associate or Covered Entity after Business Associate learns of such occurrence. Business Associates shall report within five business days of the notice to the Covered Entity: (a) identify the nature of the unauthorized use or disclosure/security incident; (b) Identify the PHI used or disclosed; (c) identify who made the unauthorized use or received the unauthorized disclosure; (d) identify what Business Associate has done or

shall do to mitigate any deleterious effect of the unauthorized use or disclosure (e) identify what corrective action Business Associate has taken or shall take to prevent future similar unauthorized use or disclosure; and (f) provide such other information, including a written report, as reasonably requested by Covered Entity.

i. With respect to the reporting of a security incident, as referenced above, the parties stipulate and agree that Business Associate will furnish the required report to Covered Entity in all cases involving a "Successful Security Incident," which is defined for purposes of this Business Associate Agreement as any security incident that results in unauthorized access, use, disclosure, modification or destruction of electronic protected health information of Covered Entity or interference with system operations adversely affecting the ability of Business Associate to maintain, process or safeguard electronic protected health information of Covered Entity. The parties further stipulate and agree that this paragraph constitutes notice by Business Associate to Covered Entity with respect to any Unsuccessful Security Incident, which is defined for purposes of this Business Associate Agreement as any security incident that does not result in unauthorized access, use, disclosure, modification or destruction of electronic protected health information of Covered Entity or interference with system operations adversely affecting the ability of Business Associate to maintain, process or safeguard electronic protected health information of Covered Entity. By way of example, such Unsuccessful Security Incidents may include: (i) pings on the firewall of Business Associate; or (ii) port scans; or (iii) attempts to log on to a system or enter a database with an invalid password or username; or (iv) denial-of-service attacks that do not result in a server being taken off-line; or (v) malware (worms, viruses, etc.). The parties further stipulate and agree that with respect to any such Unsuccessful Security Incident, no further or more detailed report to Covered Entity is needed or required under this Business Associate Agreement.

ii. In the event of an unauthorized disclosure or breach of a plan participant's PHI that is in the custody or control of Business Associate, Business Associate will take the following steps to assist Covered Entity in addressing applicable requirements under the HIPAA Rules, and to assist Covered Entity in fulfilling Covered Entity's HIPAA breach notice obligations. Within 5 business days, Business Associate agrees to provide:
    a. Business Associate's initial assessment and opinion regarding whether a particular unauthorized data release incident constitutes a "breach" that triggers the HIPAA breach notice requirements; and
    b. Business Associate's initial risk assessment and opinion regarding level of risk associated with breach.
    c. Business Associate agrees to provide Covered Entity with copies of all materials and information disclosed so that Covered Entity can perform independent risk assessment; and
    d. Where notifications are required, Business Associate agrees to provide assistance in drafting proposed notification(s) to the affected individuals,

HHS/OCR, or prominent media outlets, however, Covered Entity will make final determination and be responsible for notification of individuals, HHS/OCR and media if required, unless Business Associate is also considered a Covered Entity and the affected individuals are not solely covered under the State of Arkansas, ARBenefits health plans; and

e. Business Associate will provide assistance to Covered Entity in the form of supplying data in the possession of the Business Associate that is needed by Covered Entity to make the annual report to HHS/OCR of data breach incidents, as required under the HIPAA Rule. Business Associate agrees to work cooperatively with Covered Entity to help Covered Entity fulfill the annual HHS/OCR log or reporting requirement.

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 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 "individual or the individual's designee" as necessary to satisfy covered entity's obligations under 45 CFR 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 CFR 164.526, or take other measures as necessary to satisfy covered entity's obligations under 45 CFR 164.526;

(g) Maintain and make available the information required to provide an accounting of disclosures to the "individual" as necessary to satisfy covered entity's obligations under 45 CFR 164.528;

(h) To the extent the business associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and

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

III. **Permitted Uses and Disclosures by Business Associate**

(a) Business associate may only use or disclose protected health information as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information it creates or receives to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Request for Proposal, provided that such use or disclosure would not violate HIPAA Rules if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

(b) Business associate may request additional use of Covered Entities data by specific request, which will be reviewed and approved on an individual basis and added as an addendum to this agreement and to the Request for Proposal (underlying services agreement).

(c) Business associate may not release Covered Entities data, even in de-identified format (45 CFR 164.514(a)-(c)) without written request and authorization from Covered Entity.

(d) Business associate may use or disclose protected health information as required by law.

(e) Business associate agrees to make uses and disclosures and requests for protected health information consistent with covered entity's minimum necessary policies and procedures.

(f) Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity, except for the specific uses and disclosures set forth below.

(g) Business associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.

(h) Except as otherwise limited in this Agreement, business associate may provide data aggregation services relating to the health care operations of the covered entity as permitted by 45 CFR **-** 164.504(e)(2)(i)(B).

IV. **Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions**

(a) Covered entity shall notify business associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect business associate's use or disclosure of protected health information.

(b) Covered entity shall notify 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 business associate's use or disclosure of protected health information.

(c) Covered entity shall notify business associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate's use or disclosure of protected health information.

V. **Permissible Requests by Covered Entity**

Covered entity shall not request business associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164

if done by covered entity. Business associate may use or disclose protected health information for data aggregation or management and legal responsibilities of the business associate.

VI. **Term and Termination**

(a) Term. This Agreement shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, 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 Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section, or on the date covered entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

1. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;
2. Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or
3. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

(c) Obligations of Business Associate Upon Termination.

Upon termination of this Agreement for any reason, business associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:

1. Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;
2. Return to covered entity or, destroy the remaining protected health information that the business associate still maintains in any form;
3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic 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 business associate retains the protected health information;
4. Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at in section III “Permitted Uses and Disclosures By Business Associate” which applied prior to termination; and

5. Return to covered entity or, destroy the protected health information retained by business associate when it is no longer needed by business associate for its proper management and administration or to carry out its legal responsibilities.

(d) Survival. The obligations of business associate under this Section shall survive the termination of this Agreement.

VII. **Miscellaneous**

(a) Regulatory References. 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 as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(c) Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

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

COVERED ENTITY	BUSINESS ASSOCIATE
By: Employee Benefits Division	By:_____
Print Name:_____	Print Name:_____
Print Title:_____	Print Title:_____
Date: _____	Signature: _____
	Date:_____