Attachment F
DHS-4001 6/30/10

BUSINESS ASSOCIATE AGREEMENT

between

ARKANSAS DEPARTMENT OF HUMAN SERVICES

and

,

(Business Name)

(Business Taxpayer Identification Number)

This Business Associate Agreement ("Agreement") is made effective the_____day of _____, 2016, (the "Effective Date") by and between the Arkansas Department of Human Services ("Covered Entity") and , ("Business Associate") ("collectively the "Parties").

1. BACKGROUND

a. Covered Entity has been designated as a hybrid entity for purposes of the HIPAA Privacy Rule, and it has designated several of its component agencies as health care components.

b. In accordance with the laws of Arkansas, Business Associate provides services for Covered Entity unrelated to treatment, payment or healthcare operations and therefore the Parties believe a Business Associate Agreement is required. The provision of such services may involve the disclosure of individually identifiable health information from Covered Entity to Business Associate.

c. The relationship between Covered Entity and Business Associate is such that the Parties believe Business Associate is or may be a "business associate" within the meaning of the HIPAA Privacy Rule.

d. The Parties enter into this Agreement with the intention of complying with the HIPAA Privacy and Security Rule provisions and the Health Information Technology for Economic and Clinical Health (HITECH) Act, that a covered entity may disclose protected health information to a business associate, and may allow a business associate to create or receive protected heath information on its behalf, if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.

2. DEFINITIONS.

Unless some other meaning is clearly indicated by the context, the following terms shall have the following meaning in this Agreement:

a. "Breach" shall have the meaning set out in its definition at 45 C.F.R. § 164.402, as such provision is currently drafted and as it is subsequently updated, amended or revised.

b. "HIPAA" shall mean the Administrative Simplification Provisions, Sections 261 through 264, of the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

c. "Individual" shall have the same meaning as the term "individual" in 45 CFR 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

d. "Jurisdiction" means a geographic area smaller that a state, such as a county, city or town.

e. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

f. "Protected Health Information" ("PHI") shall have the same meaning as the term "protected health information" in 45 CFR 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

g. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR 164.103.

h. "Secretary" shall mean the Secretary of the United States Department of Health and Human Services or his designee.

i. "State" For the purpose of notification of breaches of unsecured Protected Health Information, State shall include any of the several states, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa and the Northern Mariana Islands.

j. "Unsecured Protected Health Information" shall have the meaning set out in its definition at 45 C.F.R. Section 164.402; as such provision is currently drafted and as it is subsequently updated, amended or revised.

Unless otherwise defined in this Agreement, terms used herein shall have the same meaning as those terms have in the HIPAA Privacy Rule.

3. OBLIGATIONS OF BUSINESS ASSOCIATE

In connection with this Agreement and in consideration of the mutual promises contained herein, the sufficiency of which is acknowledged by the parties, the parties hereby agree as follows:

a. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by this Agreement or as required by law.

b. Business Associate agrees to use reasonable administrative, physical and technical safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

c. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

d. Business Associate agrees to report to Covered Entity any unauthorized acquisition, access, use, or disclosure of unsecured PHI the Business Associate holds on behalf of the covered entity, including the identity of each individual who is the subject of the unsecured PHI of which it becomes aware without unreasonable delay and in no case later than ten calendar days after the discovery of the breach.

e. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity agrees to the same restrictions and conditions that apply through this Agreement to

Business Associate with respect to such information.

f. Business Associate agrees to provide access, at the request of Covered Entity, to Protected Health Information in a Designated Record Set to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR 164.524.

g. Business Associate agrees, at the request of Covered Entity, to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR 164.526.

h. Unless otherwise prohibited by law, Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, or to the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

i. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528, and to provide this information to Covered Entity or an Individual to permit such a response.

Business Associate agrees to implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the Protected Health Information that the Business Associate creates, receives, maintains or transmits on behalf of the Covered Entity.

4. PERMITTED USES AND DISCLOSURES

a. Except as otherwise limited in this Agreement or by other applicable law or agreements, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Professional Services or Technical Services Contract (“the Contract”) between the parties, provided that such use or disclosure:

1) would not violate the Privacy Rule if done by Covered Entity; or

2) would not violate the minimum necessary policies and procedures of the Covered Entity.

b. Notwithstanding the foregoing provisions, Business Associate may not use or disclose Protected Health Information if the use or disclosure would violate any term of other applicable law or agreements.

5. DISCOVERY AND NOTIFICATION OF BREACH

a. Business Associate shall implement reasonable systems, policies, and procedures for discovery of possible HIPAA violations and breaches (as defined below), and shall ensure that its workplace members and other agents are adequately trained and aware of the importance of timely reporting of possible breaches.

b. Upon the discovery of any HIPAA violation by the Business Associate or any member of its workforce, (which includes, without limitation, employees, subcontractors and agents), with respect to Protected Health Information ("PHI"), the Business Associate shall promptly perform a risk assessment

to determine whether a breach of unsecured PHI has occurred and whether or not the breach has resulted in reputation harm to the owner of the PHI as required by HITECH Act.

c. When performing such risk assessment, the Business Associate shall consider who impermissibly used or to whom the information was impermissibly disclosed and the type and amount of PHI involved, keeping in mind that many forms of health information are considered sensitive for purposes of the risk of reputational harm to an individual.

d. When performing risk assessments with respect to impermissible use or disclosure of limited data sets, which include zip codes and dates of birth, the Business Associate shall consider the risk of re-identification.

e. The Business Associate shall maintain fact specific documentation of all risk assessments performed with respect to the PHI for a minimum of six years from the date the documentation is created, and shall make such documentation available to the ADHS upon request. Such documentation shall include whether the HIPAA violation that triggered the risk assessment was or was not determined to be a breach and the reason for such determination.

f. The Business Associate shall take immediate steps to mitigate any HIPAA violation with respect to the Covered Entity's PHI that is discovered and shall provide the Covered Entity with written documentation of such steps.

g. If the Business Associate determines that a breach of unsecured PHI has occurred, the Business Associate shall notify the Covered Entity of such breach within ten calendar days.

Such notice shall include:

(i) A brief description of the occurrence, including the date of the breach and the date of discovery, if known;
(ii) To the extent possible, the identity of each individual whose unsecured PHI has been, or is reasonably believed to have been, breached;
(iii) A description of the types of unsecured PHI involved;
(iv) A brief description of what the owners of the PHI can do to protect themselves;
(v) A brief description of what the Business Associate is doing to investigate the breach, mitigate harm to affected individuals, and protect against further breaches; and
(v) Any other information that the Covered Entity reasonably believes necessary to enable it to comply with its obligations under HIPAA.

h. The Business Associate shall continue to provide the Covered Entity with any additional information related to the required disclosures that becomes available following initial notice of the breach.

1) For a breach involving unsecured PHI of more than 500 individuals of a state or jurisdiction, the Business Associate shall promptly provide notice of such breach to the Covered Entity.

2) The Business Associate agrees to maintain a log of all breaches of unsecured PHI, and to submit such log to the Secretary of Health and Human Services ("Secretary") annually, no later than 60 days

after the end of each calendar year.

3) The Business Associate agrees to maintain documentation of all breaches of unsecured PHI for a minimum of six years after the creation of the documentation, and shall make such documentation available to the Secretary upon request.

i. The Business Associate hereby agrees to indemnify and hold the Covered Entity harmless from and against all liability and costs, including attorney's fees, created by any breach resulting from the acts of its employees, agents or workforce members.

7. TERM AND TERMINATION

a. **Term**. This Agreement shall be effective as of the effective date stated above and 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 infeasible to return or destroy the Protected Health Information, protections acceptable to Covered Entity are extended to such information in accordance with the termination provisions below.

b. **Termination for Cause**. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity may, at its option, provide an opportunity for Business Associate to cure the breach or end the violation, and terminate this Agreement and the Contract

c. If Business Associate does not cure the breach or end the violation within the time specified by Covered Entity; as provided in 45 C.F.R. Section 165.504(e)(2)(iii), the Covered Entity may immediately terminate this Agreement and any related agreements, including the Contract between the Covered Entity and DHS, if the Covered Entity makes the determination that the Business Associate has breached the Business Associate Agreement and has not taken steps to cure such breach. Alternatively, the Covered Entity may choose to:

(i) provide the Business Associate with ten days written notice of the existence of an alleged material breach; and

(ii) afford the Business Associate an opportunity to cure said alleged material breach upon mutually agreeable terms.

Nonetheless, in the event that mutually agreeable terms cannot be achieved within 30 days, the Business Associate must cure said breach to the satisfaction of the Covered Entity within 30 days. Failure to cure this breach to the satisfaction of the Covered Entity is grounds for immediate termination of this Agreement. If neither termination nor a cure is feasible, Covered Entity shall report the violation to the Secretary as provided in the Privacy Rule.

d. **Effect of Termination**.

i. Except as provided in paragraph (2) of this section or in this Agreement or by other applicable law or agreements, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from

Covered Entity, or created or received by Business Associate on behalf of Covered Entity, including PHI disclosed to its agents or subcontractors pursuant to 45 C.F.R. Section I 64.504(e)(2)(I) and upon destruction of the PHI provide a Certificate of Destruction acceptable to Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information. In addition, certain provisions and requirements of the Agreement shall survive its expiration or other termination in accordance with Section 5 (e) above.

ii. In the event that Business Associate determines that destroying the Protected Health Information is not feasible, Business Associate shall provide to Covered Entity notification of the conditions that make destruction not feasible. Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

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

Business Associate: _____

By: _____

Title: _____

Date: _____