Attachment B – DOM Business Associate Agreement (BAA)
THE DIVISION OF MEDICAID
OFFICE OF THE GOVERNOR
STATE OF MISSISSIPPI

BUSINESS ASSOCIATE AGREEMENT

THIS BUSINESS ASSOCIATE AGREEMENT ("Agreement") is entered into by and between the **DIVISION OF MEDICAID IN THE OFFICE OF THE GOVERNOR**, an administrative agency of the **STATE OF MISSISSIPPI** (hereinafter "DOM"), and **XXXXXXXX**(hereinafter "Business Associate"), hereinafter collectively referred to as the Parties, and modifies any other prior existing agreement for this purpose. In consideration of the mutual promises below and the exchange of information pursuant to this Agreement and in order to comply with all legal requirements for the protection of this information, the Parties therefore agree as follows:

I. RECITALS:

DOM is a state agency that acts both as an employer and as a Health Plan for public benefit with a principal place of business at 550 High Street, Suite 1000, Jackson, MS 39201. Business Associate is a corporation qualified to do business in Mississippi with a principal place of business at **XXXXXXXX.**

1. Pursuant to the Health Insurance Portability and Accountability Act ("HIPAA") of 1996 (as amended by the Genetic Information Nondiscrimination Act ("GINA") of 2008 and the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), Title XIII of Division A, and Title IV of Division B of the American Recovery and Reinvestment Act ("ARRA") of 2009) and its implementing regulations, including 45 C.F.R. Parts 160 and 164, Subparts A and E ("Privacy Rule"), and Subparts A and C ("Security Rule"):
    1. DOM, as a Covered Entity, enters into this Agreement to obtain satisfactory assurances that Business Associate will comply with and appropriately safeguard all Protected Health Information ("PHI") created, received, maintained, or transmitted by Business Associate from or on behalf of DOM, and
    2. Certain provisions of HIPAA and its implementing regulations apply to Business Associate in the same manner as they apply to DOM and such provisions are incorporated into this Agreement.
2. DOM desires to engage Business Associate to perform certain functions, activities, or services to, for, or on behalf of DOM involving the Disclosure of PHI by DOM to Business Associate, and/or the creation, receipt, maintenance, or transmission of PHI by Business

Associate, and Business Associate desires to perform such functions, activities, or services, as set forth in the Service Agreements, and wholly incorporated herein.

II. DEFINITIONS:

1. "Breach" shall mean the acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule which compromises the security or privacy of the PHI, and subject to the exceptions set forth in 45 C.F.R. § 164.402.

2. "Business Associate" shall mean **XXXXXXXXX** including all workforce members, representatives, agents, successors, heirs, and permitted assigns.

3. "Covered Entity" shall mean the Division of Medicaid in the Office of the Governor, an administrative agency of the State of Mississippi.

4. "Data Aggregation" shall have the same meaning as the term "Data aggregation" in 45 C.F.R. § 164.501.

5. "Designated Record Set" shall have the same meaning as the term "Designated record set" in 45 C.F.R. § 164.501.

6. "Disclosure" shall have the same meaning as the term "Disclosure" in 45 C.F.R. § 160.103.

7. "DOM" shall mean the Division of Medicaid in the Office of the Governor, an administrative agency of the State of Mississippi.

8. "Health Plan" shall have the same meaning as the term "Health plan" in 45 C.F.R. § 160.103.

9. "Individual" shall have the same meaning as the term "Individual" in 45 C.F.R. § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

10. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, Subparts A and E.

11. "Protected Health Information" shall have the same meaning as the term "Protected health information" in 45 C.F.R. § 160.103..

12. "Required by Law" shall have the same meaning as the term "Required by law" in 45 C.F.R. § 164.103.

13. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his/her designee.

14. "Security Incident" shall have the same meaning as the term "Security incident" in 45 C.F.R. § 164.304.

15. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Parts 160 and 164, Subparts A and C.

16. "Service Agreements" shall mean any applicable Memorandum of Understanding ("MOU"), agreement, contract, or any other similar device, and any proposal or Request for Proposal ("RFP") related thereto and agreed upon between the Parties, entered into between DOM and Business Associate.

17. "Standard" shall have the same meaning as the term "Standard" in 45 C.F.R. § 160.103.

18. "Subcontractor" shall have the same meaning as the term "Subcontractor" in 45 C. F. R. § 160.103.

19. "Unsecured Protected Health Information" shall have the same meaning as the term "Unsecured protected health information" in 45 C.F.R. § 164.402.

20. "Use" shall have the same meaning as the term "use" in 45 C.F.R. § 160.103.

21. "Violation" or "Violate" shall have the same meaning as the terms "Violation" or "violate" in 45 C.F.R. § 160.103.

All other terms not defined herein shall have the meanings assigned in HIPAA and its implementing regulations.

III. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE:

1. Business Associate agrees to not Use or Disclose PHI other than as permitted or required by the Service Agreement or as Required by Law.

2. Business Associate shall use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic PHI to prevent use or disclosure of PHI other than as provided for by this Agreement.

3. Business Associate agrees to notify DOM without unreasonable delay and no later than seventy-two (72) hours after discovery, of any Use or Disclosure of PHI not provided for by this Agreement of which it becomes aware, and any Security Incident of which it becomes aware.

4. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in Violation of the requirements of this Agreement.

5. Business Associate agrees to notify DOM without unreasonable delay, and no later than seventy-two (72) hours after discovery of any actual or suspected Breach of Unsecured PHI, all in accordance with 45 C.F.R. § 164.410. The notification shall include, to the extent possible and subsequently as the information becomes available, the identification of all Individuals whose Unsecured PHI is reasonably believed by Business Associate to have been Breached along with any other available information that is required to be included in the notification to the Individual, HHS, and/or the media, all in accordance with the data Breach notification requirements set forth in 45 C.F.R.§ 164.410..

6. Once an actual or suspected Breach is reported to DOM, Business Associate agrees to provide a written assessment to determine whether the incident is reportable within ten (10) working days. An impermissible use or disclosure of protected health information is presumed to be a Breach unless the Covered Entity or Business Associate, as applicable, demonstrates there is a low probability the PHI has been compromised or one of the exceptions to the definition of Breach applies, all in accordance with 45 C.F.R. §164.410.

7. In accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), Business Associate agrees to 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 Business Associate with respect to such information. Business Associate agrees to ensure that any Subcontractors that create, receive, maintain, or transmit electronic PHI on behalf of Business Associate will agree to comply with the applicable requirements of the Security Rule and Privacy Rule by entering into a Business Associate Agreement and Business Associate shall provide DOM with a copy of all such executed agreements between Business Associate and Business Associate's Subcontractors at least thirty (30) calendar days prior to disclosing any of DOM's PHI pursuant to said agreements by submitting a written or electronic copy to DOM's Privacy Officer at the address included in Section VII(f) of this Agreement. Business Associate understands that submission of their Subcontractors' Business Associate Agreement(s) to DOM does not constitute DOM approval of any kind, including of the use of such Subcontractors or of the adequacy of such agreements.

8. Business Associate agrees to provide access, at the request of DOM, and in the time and manner designated by DOM, to PHI in a Designated Record Set, to DOM or, as directed by DOM, to an Individual in order to meet the requirements under 45 CFR § 164.524.

9. Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that DOM directs or agrees to pursuant to 45 CFR § 164.526 at the request of DOM or an Individual, and in the time and manner designated by DOM.

10. Business Associate agrees to document such Disclosures of PHI and information related to such Disclosures as would be required for DOM to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR § 164.528. Business

Associate agrees to retain such documentation for at least six (6) years after the date of disclosure or provide a full accounting and relevant documentation to DOM at the time of termination.

11. Business Associate agrees to provide to DOM or an Individual, in a time and manner designated by DOM, information collected in accordance with section (III)(h) of this Agreement, to permit DOM to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR § 164.528.

12. Business Associate agrees that it shall only use or disclose the minimum PHI necessary to perform functions, activities, or services for, or on behalf of, DOM as specified in the Service Agreements. Business Associate agrees to comply with any guidance issued by the Secretary on what constitutes "minimum necessary" for purposes of the Privacy Rule, and any minimum necessary policies and procedures communicated to Business Associate by DOM.

13. Business Associate agrees that to the extent that Business Associate carries out DOM's obligations under the Privacy Rule, Business Associate will comply with the requirements of the Privacy Rule that apply to DOM in the performance of such obligation.

14. Business Associate agrees to make internal practices, books, and records, including policies and procedures, available to the Secretary for purposes of determining Business Associate's and/or DOM's compliance with the Privacy Rule pursuant to 45 C.F.R. § 160.310.

15. Business Associate agrees that nothing in this Agreement shall permit Business Associate to access, store, share, maintain, transmit or use or disclose PHI in any form via any medium with any third party, including Business Associate's Subcontractors, beyond the boundaries and jurisdiction of the United States without express written authorization from DOM.

IV. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE:

1. General Use and Disclosure Provisions: Subject to the terms of this Agreement, Business Associate may Use or Disclose PHI to perform functions, activities, or services for, or on behalf of, DOM as specified in the Service Agreements, provided that such Use or Disclosure would not violate what is required by Law or the Privacy Rule if done by DOM.

2. Specific Use and Disclosure Provisions:

    1. Business Associate may use PHI, if necessary, for the proper management and administration of the Business Associate or to carry out the legal responsibilities

of the Business Associate under the Service Agreements entered into between DOM and Business Associate.

2. If Business Associate must disclose PHI pursuant to law or legal process, Business Associate shall notify DOM without unreasonable delay and at least five (5) days in advance of any disclosure so that DOM may take appropriate steps to address the disclosure, if needed.

3. Business Associate may use PHI to provide Data Aggregation services exclusively to DOM as permitted by 42 C.F.R. § 164.504(e)(2)(i)(B).

V. OBLIGATIONS OF DOM:

1. DOM shall provide Business Associate with the Notice of Privacy Practices that DOM produces in accordance with 45 C.F.R. § 164.520, attached hereto as Attachment "A" and wholly incorporated herein, as well as any changes to such Notice of Privacy Practices.

2. DOM shall notify Business Associate of any limitation(s) in its Notice of Privacy Practices to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

3. DOM 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 may affect Business Associate's use or disclosure of PHI.

4. DOM shall notify Business Associate of any restriction to the use or disclosure of PHI that DOM has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

5. Permissible Requests by DOM: DOM shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by DOM.

VI. TERM AND TERMINATION:

1. Term. For all new Service Agreements entered into between DOM and Business Associate, the effective date of this Agreement is the first day that a Business Associate is provided, or has access to, PHI. For any ongoing Service Agreements entered into between DOM and Business Associate, the effective date of this Agreement is the first day that Business Associate is provided, or has access to, PHI under the applicable Service Agreement. This Agreement shall terminate when all of the PHI provided by DOM to Business Associate, or created or received by Business Associate on behalf of DOM, is destroyed or returned to DOM, or if it is infeasible to return or destroy PHI, protections

are extended to such information, in accordance with the termination provisions of this section.

2. Termination for Cause. Upon DOM's knowledge of a material Breach or Violation by Business Associate, DOM shall, at its discretion, either:

    1. provide an opportunity for Business Associate to cure the Breach or end the Violation and terminate this Agreement and the associated Service Agreements, if Business Associate does not cure the Breach or end the Violation within the time specified by DOM, or

    2. immediately terminate this Agreement and the associated Service Agreements if Business Associate has Breached a material term of this Agreement and cure is not possible.

3. Effect of Termination.

    1. Upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI received from, or created or received by Business Associate on behalf of, DOM in accordance with Privacy and Security Rule guidelines. This provision shall apply to PHI that is in the possession of Subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.

    2. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to DOM notification of the conditions that make return or destruction infeasible. Upon notification in writing that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further Uses and Disclosures to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

VII. MISCELLANEOUS:

1. Statutory and Regulatory References. A reference in this Agreement to a section in HIPAA, its implementing regulations, or other applicable law means the section as in effect or, as amended, and for which compliance is required.

2. Amendments/Changes in Law.

    1. General. Modifications or amendments to this Agreement may be made upon mutual agreement of the Parties, in writing signed by the Parties hereto and approved as required by law. No oral statement of any person shall modify or otherwise affect the terms, conditions, or specifications stated in this Agreement.

Such modifications or amendments signed by the Parties shall be attached to and become part of this Agreement.

2. Amendments as a Result of Changes in the Law. The Parties agree to take such action as is necessary to amend this Agreement as is necessary to effectively comply with any subsequent changes or clarifications of statutes, regulations, or rules related to this Agreement. The Parties further agree to take such action as is necessary to comply with the requirements of HIPAA, its implementing regulations, and other applicable law relating to the security and privacy of PHI.

3. Procedure for Implementing Amendments as a Result of Changes in Law. In the event that there are subsequent changes or clarifications of statutes, regulations or rules relating to this Agreement, or the Parties' compliance with the laws referenced in section (VII)(c)(ii) of this Agreement necessitates an amendment, the requesting party shall notify the other party of any actions it reasonably deems are necessary to comply with such changes or to ensure compliance, and the Parties promptly shall take such actions. In the event that there shall be a change in the federal or state laws, rules or regulations, or any interpretation of any such law, rule, regulation, or general instructions which may render any of the material terms of this Agreement unlawful or unenforceable, or materially affects the financial arrangement contained in this Agreement, the Parties may, by providing advanced written notice, propose an amendment to this Agreement addressing such issues.

3. Interpretation. Any ambiguity in this Agreement shall be resolved to permit DOM to comply with HIPAA, its implementing regulations, and other applicable law relating to the security and privacy of PHI.

4. Indemnification.

1. To the fullest extent allowed by law, Business Associate shall indemnify, defend, save and hold harmless, protect, and exonerate DOM, its employees, agents, and representatives, and the State of Mississippi from and against all claims, demands, liabilities, suits, actions, damages, losses, and costs of every kind and nature whatsoever including, without limitation, court costs, investigative fees and expenses, and attorney's fees, arising out of or caused by Business Associate and/or its partners, principals, agents, and employees in the performance of or failure to perform this Agreement. In DOM's sole discretion, Business Associate may be allowed to control the defense of any such claim, suit, etc. In the event Business Associate defends said claim, suit, etc., Business Associate shall use legal counsel acceptable to DOM. Business Associate shall be solely responsible for all costs and/or expenses associated with such defense, and DOM shall be entitled to

participate in said defense. Business Associate shall not settle any claim, suit, etc. without DOM's concurrence, which DOM shall not unreasonably withhold.

2. DOM's liability, as an entity of the State of Mississippi, is determined and controlled in accordance with Mississippi Code Annotated § 11-46-1 *et seq.*, including all defenses and exceptions contained therein. Nothing in this Agreement shall have the effect of changing or altering the liability or of eliminating any defense available to the State under statute.

5. Disclaimer. DOM makes no warranty or representation that compliance by Business Associate with this Agreement, HIPAA, its implementing regulations, or other applicable law will be adequate or satisfactory for Business Associate's own purposes or that any information in Business Associate's possession or control, or transmitted or received by Business Associate, is or will be secure from unauthorized Use or Disclosure. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.

6. Notices. Any notice from one party to the other under this Agreement shall be in writing and may be either personally delivered, emailed, or sent by registered or certified mail in the United States Postal Service, Return Receipt Requested, postage prepaid, addressed to each party at the addresses which follow, or to such other addresses provided for in this Agreement, or as the Parties may hereinafter designate in writing. Any such notice shall be deemed to have been given as of the date transmitted.

For DOM: DOM Privacy Officer

Mississippi Division of Medicaid

550 High Street, Suite 1000

Jackson, MS 39201

For Business Associate: XXXXXXX

7. Severability. It is understood and agreed by the Parties hereto that if any part, term, or provision of this Agreement is by the courts or other judicial body held to be illegal or in conflict with any law of the State of Mississippi or any federal law, the validity of the remaining portions or provisions shall not be affected and the obligations of the parties

shall be construed in full force as if the Agreement did not contain that particular part, term, or provision held to be invalid.

8. Applicable Law. This Agreement shall be construed broadly to implement and comply with the requirements relating to HIPAA and its implementing regulations. All other aspects of this Agreement shall be governed by and construed in accordance with the laws of the State of Mississippi, excluding its conflicts of laws provisions, and any litigation with respect thereto shall be brought in the courts of the State. Business Associate shall comply with applicable federal, state, and local laws, regulations, policies, and procedures as now existing and as may be amended or modified. Where provisions of this Agreement differ from those mandated by such laws and regulations, but are nonetheless permitted by such laws and regulations, the provisions of this Agreement shall control.

9. Non-Assignment and Subcontracting. Business Associate shall not assign, subcontract, or otherwise transfer this Agreement, in whole or in part, without the prior written consent of DOM. Any attempted assignment or transfer of its obligations without such consent shall be null and void. No such approval by DOM of any subcontract shall be deemed in any way to provide for the incurrence of any obligation of DOM in addition to the total compensation agreed upon in this Agreement. Subcontracts shall be subject to the terms and conditions of this Agreement and to any conditions of approval that DOM may deem necessary. Subject to the foregoing, this Agreement shall be binding upon the respective successors and assigns of the parties. DOM may assign its rights and obligations under this Agreement to any successor or affiliated entity.

10. Entire Agreement. This Agreement contains the entire agreement between the Parties and supersedes all prior discussions, instructions, directions, understandings, negotiations, agreements, and services for like services.

11. No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the Parties and their respective successors, heirs, or permitted assigns, any rights, remedies, obligations, or liabilities whatsoever.

12. Assistance in Litigation or Administrative Proceedings. Business Associate shall make itself and any workforce members, contractors, subcontractors, representatives, agents, affiliates, or subsidiaries assisting Business Associate in the fulfillment of its obligations under this Agreement, available to DOM, at no cost to DOM, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against DOM, its directors, officers, or any other workforce member based upon claimed Violation of HIPAA, its implementing regulations, or other applicable law, except where Business Associate or its workforce members, contractors, subcontractors, representatives, agents, affiliates, or subsidiaries are a named adverse party.

IN WITNESS WHEREOF, the Parties hereto have duly executed this Business Associate Agreement to be effective on the date provided for in section (VI)(a) of this Agreement.

Mississippi Division of Medicaid	**Business Associate**
By: _____	**By: _____**
Drew L. Snyder	XXXXXX
Executive Director	XXXXXX
Date: _____	**Date: _____**