DATA USE AGREEMENT

In order to secure data that resides in the **Mississippi Division of Medicaid** ("DOM") system of records, whether stored electronically, on paper, or in any other medium, and to ensure the integrity, security, and confidentiality of such data and documents, and to permit only appropriate disclosure and use as may be permitted by law, the Parties below enter into this Data Use Agreement ("Agreement") to comply with the following specific sections:

I. RECITALS

a. This Agreement is by and between **DOM** and _____ ("User"), hereinafter referred to as the Parties.
b. User warrants that it is not excluded from participation in any federal or state health-care program, including Medicare and Medicaid.
c. This Agreement addresses the conditions under which DOM will disclose and User will obtain and use DOM data.
d. The Parties mutually agree that the following named person is designated as "Custodian of Data" on behalf of User and shall be responsible for the observance of all conditions of use for establishment and maintenance of security arrangements as specified in this Agreement to prevent unauthorized use or disclosure. User agrees to notify DOM within fifteen (15) business days of any change to the custodianship.

(Name and Title of Custodian of Data)	**(Company/Organization)**
(Address)	
(Phone)	**(Email address)**

e. The Parties mutually agree that the following named person will be designated as "Point-of-Contact" for this Agreement on behalf of DOM.

Glenn Swartzfager

Privacy Officer, DOM Legal Department
(601) 359-0625
glenn.swartzfager@medicaid.ms.gov

f. The Parties mutually agree that the following specified Attachments are part of this Agreement:

Attachment A:	DOM Data Elements
Attachment B:	SSA Computer Matching and Privacy Protection Act Agreement
Attachment C:	Security Controls
Attachment D:	Notification of Breach

Attachment E: Certificate of Return or Destruction/Sanitization of Confidential Data

Attachment F: Service Agreement

g. The Parties mutually agree, and in furnishing data hereunder DOM relies upon such agreement, that such data will be used solely for the following purpose, as detailed in the Service Agreement executed by the Parties **(Attachment F)**: **Contract between _____ and the Mississippi Division of Medicaid** for _____.

h. Some of the data specified in this Agreement may constitute Protected Health Information ("PHI"), Personally Identifiable Information (PII), or personal information ("PI") under federal or state law. The Parties mutually agree that the creation, receipt, maintenance, transmittal, and disclosure of DOM data containing PHI or PI shall be subject to the applicable provisions of 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), its implementing regulations, and the provisions of other applicable federal and state law.

II. DEFINITIONS

The following definitions shall apply to this Agreement.

a. "Confidential Data" shall mean any information from which an individual may be uniquely identified, including, without limitation, an individual's name, address, telephone number, social security number, birth date, account numbers, and healthcare information. Confidential information is construed broadly to include DOM data, protected health information (PHI)[1], and Personally Identifiable Information (PII)[2], which shall include all data provided to DOM by the Social Security Administration (SSA).

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

c. "DOM data" shall mean all data that is collected, stored, processed, or generated by or on behalf of DOM under this Agreement, including all attachments.

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

e. "Service Agreement" 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 User.

f. "User" shall mean _____, including all workforce members, representatives, subcontractors, agents, successors, heirs, and permitted assigns.

[1] Which shall have the same meaning as the term "Protected Health Information" in 45 C.F.R. §160.103

[2] Which is defined by the United States Government Accountability Office (GAO) as, "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as a medical, education, financial, and employment information" (NIST SP 800-122).

III. OBLIGATIONS AND ACTIVITIES OF USER

a. User represents and warrants that, except as DOM shall authorize in writing, User shall not disclose, release, reveal, show, sell, rent, lease, loan, or otherwise grant access to the data covered by this Agreement to any person, company, or organization. User agrees that, within User's organization, access to the DOM data covered by this Agreement shall be limited to the minimum number of individuals necessary to achieve the purpose stated in section (I)(g) of this Agreement and to those individuals on a need-to-know basis only.

b. Upon completion of the purpose specified in section (I)(g) of this Agreement, User shall return to DOM and/or destroy/sanitize all DOM data covered by this Agreement in accordance with the following:

   i. Return. DOM data must be returned to DOM in a sealed secure method. User will maintain a log of all DOM data being returned to DOM. All DOM data returned via 3rd party carrier will be traceable and require the signature of the receiving party.
   ii. Destruction/Sanitization. DOM data in electronic form must be sanitized (cleared or purged) in accordance with NIST Special Publication 800-88 Revision 1 or as approved in writing by DOM. Media may also be physically destroyed in accordance with NIST Special Publication 800-88 Revision 1. User shall destroy all paper documents with DOM data by using a confidential method of destruction, such as crosscut shredding or contracting with a company that specializes in confidential destruction of documents.

   User agrees that no data from DOM records, any parts or copies thereof, including data derived from DOM records (electronic, paper, or otherwise), shall be retained when the data is returned and/or destroyed/sanitized unless authorization in writing for the retention of such data has been received from the DOM signatories designated in section (VI)(c) of this Agreement. User shall certify the return and/or destruction/sanitization of the file(s) in writing using **Attachment E,** Certificate of Return or Destruction/Sanitization of Confidential Data, upon termination of the DUA. In the event that User determines that returning and/or destroying/sanitizing DOM data is infeasible, User shall provide to DOM notification of the conditions that make return and/or destruction/sanitization infeasible. Upon notification in writing that return and/or destruction of DOM data is infeasible, User shall extend the protections of this Agreement to such data and limit further uses and disclosures to those purposes that make the return and/or destruction/sanitization infeasible, for so long as User maintains such data.

c. User agrees to establish and maintain appropriate administrative, technical, and physical safeguards to protect the confidentiality of DOM data and to prevent unauthorized use or access to it. The safeguards shall provide a level and scope of security that is not less than the level and scope of security established in HIPAA and its implementing regulations. User also agrees to provide a level and scope of security that is at least comparable to the level and scope of security established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III – Security of Federal Automated Information systems, which sets forth guidelines for automated information systems in Federal agencies. If the data obtained by User from DOM includes data provided to DOM by the Social Security Administration (SSA), User shall also comply with the substantive privacy and security

requirements in the Computer Matching and Privacy Protection Act Agreement between SSA and the State of Mississippi, which is attached as **Attachment B** and incorporated into this Agreement. In addition, User agrees to comply with the specific Security Controls enumerated in **Attachment C** of this Agreement. In case of a conflict between any of the security standards contained in any of these enumerated sources of security standards, the most stringent shall apply. The most stringent means that safeguard which provides the highest level of protection to DOM data from unauthorized disclosure.

d. User acknowledges that in addition to the requirements of this Agreement, they must also abide by the applicable privacy and disclosure laws and regulations under HIPAA, the Privacy Act of 1974 (as amended by the Computer Matching and Privacy Protection Act of 1988), 42 C.F.R. Part 2, their implementing regulations, and other applicable federal and state law.
e. User agrees that all DOM data shall not be co-mingled with other trading partner's data, and shall be easily identifiable and exportable. DOM Data shall be stored in an individual structure in accordance with the following: User shall create an instance (single-tenant) of the particular database software utilized by User, and only DOM data shall reside in that instance of the database. The intent of this section is not to require separate procurement of hardware specific to DOM, however DOM data must not reside in a database that contains other entities' data.
f. User agrees that nothing in this Agreement shall permit User to access, store, share, maintain, transmit or use or disclose PHI in any form via any medium with any third party, including User's Business Associates or subcontractors, beyond the boundaries and jurisdiction of the United States without the express written authorization from DOM.
g. User agrees that all DOM data will be encrypted using industry standard algorithms as approved by DOM, in flight and at rest.
h. User agrees to comply with the State of Mississippi ITS Enterprise Security Policy, which will be provided upon request.
i. Without limitation of the foregoing:
    i. Pursuant to 42 U.S.C. § 17931(a), the following sections of the Security Rule shall apply to User as it relates to PHI in the same manner as they apply to DOM: 45 C.F.R. §§ 164.308 (Administrative Safeguards); 164.310 (Physical Safeguards); 164.312 (Technical Safeguards); and 164.316 (Policies and procedures and documentation requirements).
j. User agrees to report to DOM any use or disclosure of the information not provided for by this Agreement of which they become aware, without unreasonable delay, and no later than seventy-two (72) hours after discovery, and to take further action regarding the use or disclosure as specified in **Attachment D**, Notification of Breach, of this Agreement.
k. User agrees to mitigate, to the extent practicable, any harmful effect that is known to user of a use or disclosure of PHI, PII, or confidential information by user in Violation of the requirements of this Agreement.
l. If User must Disclose DOM data pursuant to law or the legal process, User shall notify DOM without unreasonable delay and at least ten (10) calendar days in advance of any disclosure so that DOM may take appropriate steps to address the disclosure, if needed.
m. User agrees to train and use reasonable measures to ensure compliance with the requirements of this Agreement by employees who assist in the performance of functions or activities under this Agreement and use or disclose DOM data, and to discipline such

employees who intentionally violate any provisions of this Agreement, including by termination of employment if necessary. In complying with the provisions of this section, User shall observe the following requirements:

i. User shall provide information privacy and security training, at least annually, at its own expense, to all its employees who assist in the performance of functions or activities under this Agreement and use or disclose DOM data; and
ii. User shall require each employee who receives information privacy and security training to sign a certification, indicating the employee's name and the date on which the training was completed.

n. From time to time, DOM may, upon prior written notice and at mutually convenient times, inspect the facilities, systems, books, and records of User to monitor compliance with this Agreement. User shall promptly remedy any violation of any provision of this Agreement and shall certify the same to the DOM Privacy Officer in writing. The fact that DOM inspects, or fails to inspect, or has the right to inspect, User's facilities, systems, and procedures does not relieve User of their responsibility to comply with this Agreement.

IV. TERM AND TERMINATION

a. Term. The effective date of this Agreement is the effective date of the Service Agreement entered into between DOM and User.
b. Termination. This Agreement shall terminate when all of the data provided by DOM to User is destroyed/sanitized or returned to DOM as set forth in section (III)(b) of this Agreement and a Certificate of Return or Destruction/Sanitization of Confidential Data is sent to the DOM Point-of-Contact named in section (I)(e) of this Agreement.
c. Termination for Cause. Upon DOM knowledge of a material breach or violation of this Agreement by User, DOM shall at its discretion either:
   i. provide an opportunity for User to cure the breach or end the violation and terminate this Agreement and the associated Service Agreement, if User does not cure the breach or end the violation within the time specified by DOM, or
   ii. immediately terminate this Agreement and the associated Service Agreement if User has breached a material term of this Agreement and cure is not possible.
d. Effect of Termination. Upon termination of this Agreement, for any reason, User shall return to DOM and/or destroy/sanitize all DOM data in accordance with section (III)(b) of this Agreement. The provisions of this Agreement governing the privacy and security of DOM data shall remain in effect until all data is returned and/or destroyed/sanitized and DOM receives a Certificate of Return or Destruction/Sanitization of Confidential Data from User.

V. MISCELLANEOUS

a. Penalties. User acknowledges that criminal, administrative, and civil penalties under HIPAA, the Privacy Act, 42 C.F.R. Part 2, their implementing regulations, and other applicable federal and state law, may apply with respect to any use or disclosure of information or data that is inconsistent with the terms of this Agreement. By signing this Agreement, User agrees to abide by all provisions set out in this Agreement, including all attachments, for protection of the data specified in this Agreement, and acknowledges

having received notice of potential criminal, administrative, or civil penalties for violation of the terms of the Agreement. User agrees any material violations of the terms of this Agreement or any of the laws and regulations governing the use of DOM data may result in denial of access to DOM data.

b. Statutory and Regulatory References. A reference in this Agreement to HIPAA, the Privacy Act, 42 C.F.R. Part 2, their implementing regulations, or other applicable federal and state law means the section as in effect or as amended, and for which compliance is required.

c. Amendments/Changes in Law.
   i. *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.
   ii. *Amendments as a Result of Changes in the Law.* The Parties agree to take such action as is necessary to amend this Agreement 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 applicable requirements of HIPAA, the Privacy Act, 42 C.F.R. Part 2, their implementing regulations, and any other applicable federal and state law relating to the security and privacy of DOM data.
   iii. *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 (V)(c)(ii) of this Agreement necessitates an amendment, the requesting party shall notify the other party of the need for an amendment or 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.

d. Survival. The respective rights and obligations of User under section (IV)(d) of this Agreement shall survive the termination of this Agreement.

e. Interpretation. Any ambiguity in this Agreement shall be resolved to permit DOM to comply with HIPAA, the Privacy Act, 42 C.F.R. Part 2, their implementing regulations, and any other applicable federal or state law. The Parties agree that instructions or interpretations issued to User concerning this Agreement, and the data and documents specified herein, shall not be valid unless issued in writing by the DOM Point-of-Contact specified in section (I)(d) of this Agreement or the DOM signatories to this Agreement shown in section (VI)(c) of this Agreement.

f. Indemnification. To the fullest extent allowed by law, User 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 User and/or its partners, principals, agents, and employees in the performance of or failure to perform this Agreement. In DOM's sole discretion, User may be allowed to control the defense of any such claim, suit, etc. In the event User defends said claim, suit, etc., User shall use legal counsel acceptable to DOM. User shall be solely responsible for all costs and/or expenses associated with such defense, and DOM shall be entitled to participate in said defense. User shall not settle any claim, suit, etc. without DOM's concurrence, which DOM shall not unreasonably withhold.

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.

g. Disclaimer. DOM makes no warranty or representation that compliance by User with this Agreement, HIPAA, the Privacy Act, 42 C.F.R. Part 2, their implementing regulations, and other applicable laws and regulations will be adequate or satisfactory for User's own purposes or that any information in User's possession or control, or transmitted or received by User, is or will be secure from unauthorized use or disclosure. User is solely responsible for all decisions made by User regarding the safeguarding of DOM data.

h. 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:

DOM: **Office of the Governor**
Division of Medicaid
550 High Street, Suite 1000
Jackson, MS 39201

User: _____
_____
_____
_____

Any such notice shall be deemed to have been given as of the date transmitted.

i. 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.

j. Applicable Law. This Agreement shall be construed broadly to implement and comply with the privacy and security requirements of HIPAA, the Privacy Act, 42 C.F.R. Part 2, their implementing regulations, and other applicable federal and state law. 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. User 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.

k. Non-Assignment and Subcontracting. User shall not assign, subcontract, or otherwise transfer this Agreement, in whole or in part, without the prior written consent of DOM, and provided that User provides DOM with a list of all such subcontractors, and submits an updated list upon any subsequent change. 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.

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

m. 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.

n. Assistance in Litigation or Administrative Proceedings. User shall make itself and any workforce members, contractors, subcontractors, agents, representatives, subsidiaries, or affiliates assisting User 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, the Privacy Act, 42 C.F.R. Part 2, their implementing regulations, or other laws relating to security and privacy, except where User or its workforce members, contractors, subcontractors, agents, representatives, subsidiaries, or affiliates are a named adverse party.

[Remainder of page intentionally left blank; signature page follows.]

VI. ACKNOWLEDGEMENTS AND ATTESTATIONS

a. **The Custodian of Data**, as named in section (I)(d) of this Agreement, hereby acknowledges his/her appointment as Custodian of the aforesaid data on behalf of User, and agrees in a representative capacity to comply with all of the provisions of this Agreement on behalf of User.

(Name of Custodian of Data – Typed or Printed) **(Title/Component)**

(Signature) **(Date Signed – mm/dd/yyyy)**

b. **On behalf of User**, the undersigned person hereby attests that he/she is authorized to enter into this Agreement and agrees to all the terms specified herein.

(Name – Typed or Printed) **(Title/Component)**

(Company/Organization) **(User NPI Number- If Applicable)**

(Address)

(Phone Number) **(Email Address)**

(Signature) **(Date Signed – mm/dd/yyyy)**

c. **On behalf of DOM**, the undersigned person hereby attests that he/she is authorized to enter into this Agreement and agrees to all the terms specified herein.

Cindy Bradshaw **Executive Director**

(Signature) **(Date Signed – mm/dd/yyyy)**