Attachment C to RFP No. 4111 – DOM Data Use Agreement (DUA)
<u>DATA USE AGREEMENT</u>

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.

Rita Rutland
Deputy Administrator, Office of Information Technology
(601) 576-4147
rita.rutland@medicaid.ms.gov

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

Attachment A:	DOM Data
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 the Division of Medicaid in the Office of the Governor State of Mississippi and _____ 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.

---

[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).

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

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   AES with 256 bit keys SSL v3.0/TLS v1.2 or better at all times (i.e., whether data is in transit or 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. <u>Term</u>. The effective date of this Agreement is the effective date of the Service Agreement entered into between DOM and User.

b. <u>Termination</u>. 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. <u>Termination for Cause</u>. 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. <u>Effect of Termination</u>. 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. <u>Penalties</u>. 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. <u>Statutory and Regulatory References</u>. 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. <u>Amendments/Changes in Law</u>.

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

e. <u>Interpretation</u>. 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.

MS DOM DUA Revised 2018

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.

Drew L. Snyder   **Executive Director**

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

Data Use Agreement

Attachment A – DOM Data

This is a post award document.

**RENEWAL OF THE COMPUTER MATCHING AGREEMENT
BETWEEN
THE SOCIAL SECURITY ADMINISTRATION
AND
THE STATE OF MISSISSIPPI**

SSA Match #6000

Under the applicable provisions of the Privacy Act of 1974, amended by the Computer Matching
and Privacy Protection Act of 1988, 5 U.S.C. § 552a(o)(2), a computer matching agreement will
remain in effect for a period not to exceed 18 months. Within 3 months prior to the expiration of
such computer matching agreement, however, the Data Integrity Board (DIB) may, without
additional review, renew the computer matching agreement for a current, ongoing matching
program for a period not to exceed 12 additional months if:

1. such program will be conducted without any changes; and

2. each party to the Agreement certifies to the DIB in writing that the program has been
   conducted in compliance with the Agreement.

The following match meets the conditions for renewal upon signature of the officials authorized
in sections VII and VIII of this renewal:

I. TITLE OF MATCH:

   Computer Matching and Privacy Protection Act Agreement Between the Social Security
   Administration and the State of Mississippi (Match #6000)

II. PARTIES TO THE MATCH:

   Recipient Agency: Mississippi (State)

   Source Agency: Social Security Administration (SSA)

III. PURPOSE OF THE AGREEMENT:

   This Agreement between SSA and the State sets forth the terms and conditions governing
   disclosures of records, information, or data (collectively referred to herein as "data")
   made by SSA to various State agencies and departments (State Agencies) that administer
   federally funded benefit programs, including those under various provisions of the Social
   Security Act (Act), such as section 1137 (42 U.S.C. § 1320b-7), as well as the state-
   funded state supplementary payment programs under Title XVI of the Act. The terms
   and conditions of this Agreement ensure that SSA makes such disclosures of data, and
   the State uses such disclosed data, in accordance with the requirements of the Privacy Act
   of 1974, as amended by the CMPPA of 1988, 5 U.S.C. § 552a.

Under section 1137 of the Act, the State is required to use an income and eligibility verification system to administer specified federally funded benefit programs, including the state-funded state supplementary payment programs under Title XVI of the Act. To assist the State in determining entitlement to and eligibility for benefits under those programs, as well as other federally funded benefit programs, SSA discloses certain data about applicants (and in limited circumstances, members of an applicant's household), for state benefits from SSA Privacy Act Systems of Records and verifies the Social Security numbers of the applicants.

IV. ORIGINAL EFFECTIVE AND EXPIRATION DATES OF THE MATCH:

Effective Date: July 1, 2017
Expiration Date: December 31, 2018

V. RENEWAL AND NEW EXPIRATION DATES:

Renewal Date: January 1, 2019
New Expiration Date: December 31, 2019

VI. SOCIAL SECURITY ADMINISTRATION SIGNATURES:
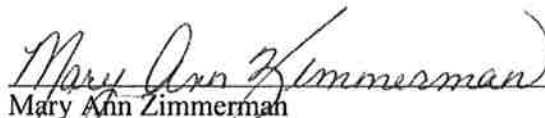
Source Agency Certification:

As the authorized representative of the source agency named above, I certify that: (1) the subject matching program was conducted in compliance with the existing computer matching agreement between the parties; and (2) the subject matching program will continue without any changes for an additional 12 months, subject to the approval of the respective Data Integrity Boards of the parties.

Electronic Signature Acknowledgement: If using an electronic signature, by clicking the SIGN button, you are signing the document electronically. You agree that your electronic signature has the same legal validity and effect as your handwritten signature on the document, and that it has the same meaning as your handwritten signature.

Rose Mary Buehler

Date   11/1/18

Data Integrity Board Certification:

As Chair of the Data Integrity Board of the source agency named above, I certify that: (1) the subject matching program was conducted in compliance with the existing computer matching agreement between the parties; and (2) the subject matching program will continue without any changes for an additional 12 months.

Mary Ann Zimmerman
Acting Chair
Data Integrity Board

Date   August 1, 2018

VII. <u>STATE OF MISSISSIPPI SIGNATURES</u>:

<u>Recipient Agency Certification</u>:

As the authorized representative of the recipient agency named above, I certify that:
(1) the subject matching program was conducted in compliance with the existing
computer matching agreement between the parties; and (2) the subject matching program
will continue without any changes for an additional 12 months, subject to the approval of
the respective Data Integrity Boards of the parties.

Electronic Signature Acknowledgement: If using an electronic signature, by clicking the
SIGN button, you are signing the document electronically. You agree that your electronic
signature has the same legal validity and effect as your handwritten signature on the
document, and that it has the same meaning as your handwritten signature.

Phil Bryant
Governor

Date Oct. 26, 2018

DATA USE AGREEMENT

Attachment C

Security Controls

I.   Personnel Controls

A.   *Employee Training.* All workforce members who assist in the performance of functions or activities on behalf of DOM, or access or disclose DOM data must complete information privacy and security training, at least annually, at User's expense. Each workforce member who receives information privacy and security training must sign a certification, indicating the member's name and the date on which the training was completed. These certifications must be retained for a period of six (6) years following contract termination.

B.   *Employee Discipline.* Appropriate sanctions must be applied against workforce members who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment where appropriate.

C.   *Confidentiality Statement.* All persons that will be working with DOM data must sign a confidentiality statement that includes, at a minimum, General Use, Security and Privacy Safeguards, Unacceptable Use, and Enforcement Policies. The statement must be signed by the workforce member prior to access to DOM data. The statement must be renewed annually. The User shall retain each person's written confidentiality statement for DOM inspection for a period of six (6) years following contract termination.

D.   *Background Check.* Before a member of the workforce may access DOM data, a background screening of that worker must be conducted. The screening should be commensurate with the risk and magnitude of harm the employee could cause, with a more thorough screening being done for those employees who are authorized to bypass significant technical and operational security controls. The User shall retain each workforce member's background check documentation for a period of three (3) years following contract termination.

II.   Technical Security Controls

A.   *Workstation/Laptop/Tablet encryption.* All workstations, tablets and laptops that process and/or store DOM PHI or PI must be encrypted using a FIPS 140-2 certified algorithm of 256 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk unless approved by the DOM.

B.   *Server Security.* Servers containing unencrypted DOM data must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review.

C.   Co-Mingling of Data. 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.

D.   ***Minimum Necessary.*** Only the minimum necessary amount of DOM data required to perform necessary business functions may be copied, downloaded, or exported.

E.   ***Removable media devices.*** All electronic files that contain DOM data must be encrypted when stored on any removable media or portable device (i.e., USB thumb drives, CDs/DVDs, Mobile Phones, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm of 256 bit or higher, such as AES.

F.   ***Antivirus software.*** All workstations, laptops and other systems that process and/or store DOM data must install and actively use comprehensive anti-virus software solution with automatic updates scheduled at least daily.

G.   ***Patch Management.*** All workstations, laptops and other systems that process and/or store DOM data must have critical security patches applied, with system reboot if necessary. There must be a documented patch management process which determines installation timeframe based on risk assessment and vendor recommendations. At a maximum, all applicable patches must be installed within thirty (30) days of vendor release. Applications and systems that cannot be patched due to operational reasons must have compensatory controls implemented to minimize risk, where possible.

H.   ***User IDs and Password Controls.*** All users must be issued a unique user name for accessing DOM data. Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password, at maximum within twenty-four (24) hours. User IDs shall be, purged after ninety (90) days of inactivity. Passwords are not to be shared. Passwords must be at least eight (8) characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every thirty (30) days. Passwords must conform to the following guidelines:

- Passwords must contain at least eight (8) characters.
- Passwords must contain a combination of lower case letters, upper case letters, numbers, and at least one (1) symbol.
- Minimum password age of 1 day.
- Maximum password age of 60 days.
- Enforce at least four (4) changed characters when new passwords are created.
- Prohibit password reuse for 24 generations.
- Passwords must not contain the user ID.
- Passwords must not include personal information about the user that can be easily guessed: user's name, spouse's name, kid's name, employee number, social security number, birth date, telephone number, city, etc.
- Passwords must not include words from an English dictionary or foreign-language dictionary.
- Passwords must not contain any simple pattern of letters or numbers such as "qwertyxx", "12345678", or "xyz123xx."

Two Factor Authentication (2FA) is preferred.

I.   ***Data Destruction/Sanitization.*** DOM data in electronic form must be sanitized (cleared or purged) in accordance with NIST Special Publication 800-88 Rev.1 or as approved in writing by DOM. Media may also be physically destroyed in accordance with NIST Special Publication 800-88 Rev.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 document.

J. ***System Timeout.*** The system providing access to DOM data must provide an automatic timeout, requiring re-authentication of the user session after no more than 20 minutes of inactivity.

K. ***Warning Banners.*** All systems providing access to DOM data must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.

L. ***System Logging.*** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for DOM data, or which alters DOM data. The audit trail must be date and time stamped, must log both successful and failed accesses, must be read only, and must be restricted to authorized users. If DOM data is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least three (3) years after occurrence.

M. ***Access Controls.*** The system providing access to DOM data must use role based access controls for all user authentications, enforcing the principle of least privilege.

N. ***Transmission encryption.*** All data transmissions of DOM PHI or PII outside the secure internal network must be encrypted using TLS 1.2 SHA-256 or higher encryption. This requirement pertains to any type of PHI or PII in motion including, but not limited to, website access, file transfer, and E-Mail.

O. ***Intrusion Detection.*** All systems involved in accessing, holding, transporting, and protecting DOM data that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

III. Audit Controls

A. ***System Security Review.*** User must ensure audit control mechanisms that record and examine system activity are in place. All systems processing and/or storing DOM data must have at least an annual system risk assessment/security review which provides assurance that administrative, physical, and technical controls are functioning effectively and providing adequate levels of protection. Reviews should include vulnerability scanning tools. A system risk assessment/security review must be done if a change to the boundaries of the system has occurred before the annual system risk assessment/security review is scheduled to be performed.

B. ***Log Reviews.*** All systems processing and/or storing DOM data must have a routine procedure in place to review system logs for unauthorized access.

C. ***Change Control.*** All systems processing and/or storing DOM data must have a documented change control procedure that ensures separation of duties and protects the confidentiality, integrity, and availability of data.

IV. Business Continuity / Disaster Recovery Controls

A. ***Emergency Mode Operation Plan.*** User must establish a documented plan to enable continuation of critical business processes and protection of the security of electronic DOM data in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than twenty-four (24) hours.

B. ***Data Backup Plan.*** User must have established documented procedures to backup DOM data to maintain retrievable exact copies of DOM data. The plan must include a regular schedule for making backups, storing backups offsite, an inventory of backup media, and

an estimate of the amount of time needed to restore DOM data should it be lost. At a minimum, the schedule must be a weekly full backup and monthly offsite storage of DOM data.

V.   Paper Document Controls

A.   ***Supervision of Data.*** DOM PHI or PII in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. DOM PHI or PII in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

B.   ***Escorting Visitors.*** Visitors to areas where DOM PHI or PII is contained shall be escorted and DOM PHI or PII shall be kept out of sight while visitors are in the area.

C.   ***Confidential Destruction.*** DOM data must be disposed of through confidential means, such as cross cut shredding and pulverizing.

D.   ***Removal of Data.*** DOM data must not be removed from the premises of the User except with express written permission of DOM.

E.   ***Faxing.*** Faxes containing DOM PHI or PII shall not be left unattended and fax machines shall be in secure areas. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them. Fax numbers shall be verified with the intended recipient before sending the fax.

F.   ***Mailing.*** Mailings of DOM data shall be sealed and secured from damage or inappropriate viewing of PHI or PII to the extent possible. Mailings which include five hundred (500) or more individually identifiable records in a single package shall be sent using a tracked mailing method which includes verification of delivery and receipt, unless the prior written permission of DOM to use another method is obtained.

DATA USE AGREEMENT

Attachment D

Notification of Breach

I. **Definitions.** All terms used in this Attachment D, but not otherwise defined, shall have the same meanings as assigned to those terms in the Data Use Agreement ("Agreement") to which this Attachment D is incorporated.

II. **Breaches and Security Incidents.** During the term of the Agreement, User agrees to implement reasonable systems for the discovery and prompt reporting of any actual or suspected breach or security incident. "Security Incident" shall have the same meaning as defined under HIPAA and its implementing regulations (45 C.F.R. §164.304). User agrees to take the following steps:

   A. *Notice to DOM.* (1) To notify the DOM Data Use Agreement Point-of-Contact, DOM Security Officer, and DOM Privacy Officer **without unreasonable delay, and no later than seventy-two (72) hours after discovery by telephone call plus email, fax, or registered or certified mail** upon the discovery of an actual or suspected breach of unsecured PHI or PI in electronic media or in any other media. (2) To notify the DOM Data Use Agreement Point-of-Contact, DOM Security Officer, and DOM Privacy Officer **without unreasonable delay, and no later than seventy-two (72) hours after discovery by telephone call plus email, fax, or registered or certified mail** of any actual or suspected Security Incident affecting this Agreement, including but not limited to an actual or suspected security incident that involves data provided to DOM by the Social Security Administration. A breach or Security Incident shall be treated as discovered by User as of the first day on which the breach or Security Incident is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach or Security Incident) who is a workforce member, officer, or other agent of User.

   The notification shall include, to the extent possible and subsequently as the information becomes available, the identification of all individuals whose unsecured PHI or PI is reasonably believed by User to have been affected by the breach or Security Incident 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 42 U.S.C. § 17932 and 45 C.F.R. Parts 160 and 164, Subparts A, D, and E, or any other applicable notification requirements.

   Upon discovery of an actual or suspect breach or Security Incident User shall take:

   1. Prompt corrective action to mitigate any risks or damages involved with the breach or Security Incident and to protect the operating environment; and
   2. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

   B. *Investigation and Investigation Report.* To immediately investigate any such actual or suspected breach or Security Incident and to submit updated information by email, fax, or registered or certified mail as it becomes available to the DOM Data Use Agreement Point-of-Contact, DOM Security Officer, and DOM Privacy Officer.

C. *Complete Report*. To provide a complete written report by email, fax, or registered or certified mail of the investigation to the DOM Data Use Agreement Point-of-Contact, DOM Security Officer, and DOM Privacy Officer within ten (10) working days of the discovery of any actual or suspected breach or Security Incident. The report shall include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the breach or Security Incident. If DOM requests information in addition to that provided in the written report, User shall make reasonable efforts to provide DOM with such information. If necessary, a supplemental report may be used to submit revised or additional information after the completed report is submitted.

D. *Notification of Individuals*. If the cause of an actual breach of PHI or PI is attributable to User or its subcontractors, agents or vendors, User shall notify each individual of the breach when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. The notifications shall comply with the requirements set forth in 42 U.S.C. § 17932 and its implementing regulations. The DOM Data Use Agreement Point-of-Contact, DOM Security Officer, and DOM Privacy Officer shall approve the time, manner, and content of any such notifications and their review and approval must be obtained before the notifications are made.

E. *Responsibility for Reporting of Breaches.* If the cause of a breach of PHI or PI is attributable to User or its agents, subcontractors, or vendors, and User is a covered entity as defined under HIPAA and the HIPAA regulations, User is responsible for all required reporting of the breach as specified in 42 U.S.C. § 17932 and its implementing regulations, including notification to media outlets and to the Secretary of the U.S. Department of Health and Human Services. If User has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to DOM in addition to User, User shall notify DOM, and DOM and User may take appropriate action to prevent duplicate reporting. The breach reporting requirements of this paragraph are in addition to the reporting requirements set forth above.

III. *Contact Information*. To direct communications to the above referenced staff, User shall initiate contact as indicated herein. The parties reserve the right to make changes to the contact information below by giving written notice to User. Said changes shall not require an amendment to this Attachment or the Agreement to which it is incorporated.

DOM Point-of-Contact: See Data Use Agreement to which this Attachment is incorporated.

DOM Security Officer:	Address:	550 High Street, Suite 1000, Jackson, MS 39201
	Email:	securityofficer@medicaid.ms.gov
	Telephone:	(601) 359-6405
	Fax:	(601)-359-6294

DOM Privacy Officer:	Address:	550 High Street, Suite 1000, Jackson, MS 39201
	Email:	privacyofficer@medicaid.ms.gov
	Telephone:	(601) 359-6097
	Fax:	(601)-359-6294

DOM DATA USE AGREEMENT

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

I, _____ (Custodian of Data), hereby certify

the following to be true and correct:

I.   I am employed by _____ (User) as a(n)

                                                (occupation/title).

II.   Pursuant to the **Data Use Agreement** ("Agreement") to which this **Attachment E** is incorporated between the Mississippi Division of Medicaid ("DOM") and (User), I received and acted as custodian of the DOM Data described in **Attachment A** of the Agreement.

III.   The purpose for receiving the DOM Data described in **Attachment A** has been met.

      OR

      The purpose for receiving some of the DOM Data described in **Attachment A** has been met. That data is specified as follows:

IV.   In compliance with **section (III)(b) of the Agreement**, the DOM Data indicated in **section (III) of this Certificate of Return or Destruction/Sanitization of Confidential Data** has been returned to DOM by the following method of return:

      OR has been destroyed/sanitized by the following method of destruction/sanitization:

      on the following date: _____ .

V.   **IN WITNESS WHEREOF,** _____ (User) has caused this Certificate to be executed by its authorized representative as follows:

    By: _____ (Signature)
                                (Custodian of Data)
                                (Occupation/Title)

    Date: _____

Data Use Agreement

Attachment F – Service Agreement

This is a post award document.