MISSISSIPPI DIVISION OF MEDICAID

DATA USE AGREEMENT

In order to secure data and documents that reside in the Mississippi Division of Medicaid ("DOM") system of records 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 **Mississippi State Department of Health** ("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 as set out in Attachment A.

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) days of any change to the custodianship.

Lei Zhang **Office Director II**

Mississippi State Department of Health **570 East Woodrow Wilson, Jackson, MS 39215**

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

Rita Rutland **Dep. Admin., 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:	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 of Confidential Data
Attachment F:	Service Agreement(s)

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(s)

executed by the Parties (Attachment F): **Memorandum of Understanding between the Division of Medicaid in the Office of the Governor State of Mississippi and the Mississippi State Department of Health made effective February 1, 2014 for the purpose of establishing, supporting, and promoting a collaborative effort to coordinate maternal and infant vital records date for "research purposes". Such "research purposes" authorized under this Agreement only includes uses and disclosures as allowed under 45 C.F.R. § 164.512(b)(Uses and disclosures for public health activities), and does not include uses and disclosures described in 45 C.F.R. § 164.512(i)(Uses and disclosures for research purposes).**

h. Some of the data specified in this Agreement may constitute Protected Health Information ("PHI") 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 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. "DOM" shall mean the Division of Medicaid in the Office of the Governor, an administrative agency of the State of Mississippi.

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

c. "Service Agreement(s)" 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.

d. "User" shall mean Mississippi State Department of Health, 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 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 or destroy all DOM data covered by this Agreement.

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. DOM data must be destroyed by wiping such data using Department of Defense standards or as approved by DOM. 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, hardcopy, or otherwise), shall be retained when the data is returned or destroyed 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 or destruction of the file(s) in writing using Attachment E, Certificate of Return or Destruction of Confidential Data, upon renewal or termination of the DUA. In the event that User determines that returning or destroying DOM data is infeasible, User shall provide to DOM notification of the conditions that make return or destruction infeasible. Upon notification in writing that return 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 or destruction 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 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 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.

f. If User must Disclose PHI pursuant to law or the legal process, User 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.

g. 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. 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.

h. 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. Unless otherwise specified in this Agreement, for all new applicable Service Agreement(s) entered into between DOM and User, the effective date of this Agreement is the effective date of the Service Agreement(s) entered into between DOM and User. For all ongoing applicable Service Agreement(s) entered into between DOM and User, the effective date of this Agreement is the date first written in section (VI) of this Agreement.

b. Termination. This Agreement shall terminate when all of the data provided by DOM to User is destroyed or returned to DOM as set forth in section (III)(b) of this Agreement and a Certificate of Return or Destruction 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(s), 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(s) 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 or destroy 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 or destroyed and DOM receives a Certificate of Return or Destruction 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 and in Attachments B and C 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 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, 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 PHI.

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 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. User will indemnify and hold harmless DOM to this Agreement from and against all claims, losses, liabilities, costs, and other expenses incurred as a result of or arising directly or indirectly out of or in conjunction with:

   i. any misrepresentation, breach of warranty, or non-fulfillment of any undertaking on the part of User under this Agreement, and

   ii. any claims, demands, awards, judgments, actions, and proceedings made by any person or organization arising out of or in any way connected with the performance of User under this Agreement.

   iii. 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 required to be given pursuant to the terms and provisions of 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: **Lei Zhang**
Dick Johnson
Charlene Collier
Mississippi State Department of Health
570 East Woodrow Wilson
Jackson, MS 39215

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

i. Severability. In the event any provision of this Agreement is held to be unenforceable for any reason, the unenforceability thereof shall not affect the remainder of this Agreement, which shall remain in full force and effect and enforceable in accordance with its terms.

j. Governing 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 under the laws of the State of Mississippi. 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. Assignment/Subcontracting. This Agreement shall inure to the benefit of and be binding upon the Parties hereto and their respective successors, heirs, and permitted assigns. Except as otherwise provided in the Service Agreement(s), User may not assign or subcontract the rights or obligations under this Agreement without the express written consent of DOM, provided that any subcontractor executes a separate Data Use Agreement with DOM. User agrees to ensure that all agents, including a subcontractor, to whom User provides DOM data, agree to the same requirements of this Agreement and applicable laws and regulations that apply to User with respect to such information. 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, assignees, 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, assignees, subsidiaries, or affiliates are a named adverse party.

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.

Lei Zhang, PhD, MSc, MBA	Office Director
(Name of Custodian of Data – Typed or Printed)	(Title/Component)
Lei Zhang	4/30/2015
(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.

Mary Currier, MD, MPH	State Health Officer
(Name – Typed or Printed)	(Title/Component)
MS State Department of Health	
(Company/Organization)	(User NPI Number – If Applicable)
P. O. Box 1700, 570 E. Woodrow Wilson, Jackson, MS 39215-1700	
(Address)	
601-576-7634	Mary.Currier@msdh.ms.gov
(Phone Number)	(Email Address)
Mary Currier	6/2/15
(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.

David J. Dzielak, Ph.D.	Executive Director
David J. Dzielak	4/21/15
(Signature)	(Date Signed – mm/dd/yyyy)

MISSISSIPPI DIVISION OF MEDICAID

DATA USE AGREEMENT

Attachment A

Data File(s)

Data will be retrieved and saved in a flat file by DOM and transferred to User through password protected CDs or secured FTPs.

The recipient file includes the following:

Field Name	Description
ben_sys_id	Internal beneficiary system id
fst_nam	Recipient's First Name
mi_nam	Recipient's Middle Initial
last_nam	Recipeint's Last Name
ssn_num	Recipient's Social Security Number
dob_dt	Recipient's Date of Birth
race_cd	Race Code - See Valid Values tab
geo_cnty_cd	Recipient's Current County of Residence - see Valid Values tab
begin_date	Recipient's Eligibility Begin Date
end_date	Recipient's Eligibility End Date

These fields are used for matching to the birth certificate. Once the match is completed, User returns the beneficiary system ID and the date of birth to DOM and DOM pulls all of the claims for that ID that occurred during a period nine (9) months before the birth to three (3) months after the birth.

The claims file includes the following:

Field Name	Description
year_of_birth	provided in match file
cert_num	provided in match file
date_of_birth	provided in match file
ben_sys_id	Internal beneficiary system id
fst_nam	Recipient's First Name

mi_nam	Recipient's Middle Initial
last_nam	Recipeint's Last Name
ssn_num	Recipient's Social Security Number
dob_dt	Recipient's Date of Birth
race_cd	Race Code - See Valid Values tab
geo_cnty_cd	Recipient's Current County of Residence - see Valid Values tab
hdr_clnt_age	Recipient's Age on the Claim
coe_cd	Recipient's Category of Eligibility at time of service - see Valid Values tab
tcn_num	Transaction Control Number - the unique claim identifier
hdr_ty_cd,	Claim Type - see Valid Values tab
cos_cd,	State Category of Service - see Valid Values tab
pl_of_svc_cd	Place of Service - on HCFA 1500 only - see Valid Values tab
hdr_svc_fst_dt	Header First Date of Service
hdr_svc_lst_dt	Header Last Date of Service
prin_diag_cd	Principle Diagnosis Code - Institutional claims only
diag_cd1	Other Diagnosis Code 1
diag_cd2	Other Diagnosis Code 2
diag_cd3	Other Diagnosis Code 3
diag_cd4,	Other Diagnosis Code 4
prin_icd9_cd	ICD9 Surgical Principle Procedure Code
prin_icd9_dt	Date of ICD9 Surgical Principle Procedure Code
icd9_cd1	ICD9 Surgical Procedure Code 1
icd9_dt1	Date of ICD9 Surgical Procedure Code 1
icd9_cd2	ICD9 Surgical Procedure Code 2
icd9_dt2	Date of ICD9 Surgical Procedure Code 2
icd9_cd3	ICD9 Surgical Procedure Code 3
icd9_dt3	Date of ICD9 Surgical Procedure Code 3
tot_reimb_amt	Header Paid Amount - this is the total amount paid for the claim. This will be populated on Line 1 only
li_num	Claim Line number
proc_cd	CPT/HCPCs code
rev_cd	Revenue Code

li_fst_dos_dt	Line First Date of Service
li_lst_dos_dt	Line Last Date of Service
li_reimb_amt	Line Paid Amount
type	FFS or Encounter - indicates if the claim is a Medicaid Fee-for-Service claim or a Managed Care encounter claim

Access by User to the above listed data shall be granted in a time and manner determined by DOM to be in the best interest of the State, taking into consideration this Agreement and applicable federal and state law, regulations, policies, and procedures.

MISSISSIPPI DIVISION OF
MEDICAID

PHIL BRYANT
GOVERNOR

April 5, 2012

Attachment B

Mr. Brooks Hansen
Social Security Administration
1200 Rev. Abraham Woods Jr., Blvd.
2nd Floor – BITT
Birmingham, AL 35285

Dear Mr. Hansen:

Enclosed please find the Computer Matching and Privacy Protection Act data exchange agreement signed by Governor Phil Bryant on April 2, 2012.

Sincerely,

Bobby Waites
Chief Counsel

bcc: David Dzielak
Richard Berry
Mark Henry

RECEIVED
APR 06 2012
DIVISION OF MEDICAID
EXECUTIVE DIVISION

COMPUTER MATCHING AND PRIVACY PROTECTION ACT AGREEMENT BETWEEN THE SOCIAL SECURITY ADMINISTRATION AND THE STATE OF MISSISSIPPI

I. Purpose and Legal Authority

A. Purpose

This Computer Matching and Privacy Protection Act (CMPPA) Agreement between the Social Security Administration (SSA) and the State of **Mississippi** (State), sets forth the terms and conditions governing disclosures of records, information, or data (collectively referred to herein "data") made by SSA to various State agencies and departments (State Agencies) that administer federally funded benefit programs under various provisions of the Social Security Act (Act), such as section 1137 (42 U.S.C. § 1320b-7), including 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 Computer Matching and Privacy Protection Act 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 for state benefits from SSA Privacy Act Systems of Records (SOR) and verifies the Social Security numbers (SSN) of the applicants.

B. Legal Authority

SSA's authority to disclose data and the State's authority to collect, maintain, and use data protected under SSA SORs for specified purposes is:

- Sections 1137, 453, and 1106(b) of the Act (42 U.S.C. §§ 1320b-7, 653, and 1306(b)) (income and eligibility verification data);
- 26 U.S.C. § 6103(l)(7) and (8) (tax return data);
- Section 202(x)(3)(B)(iv) of the Act (42 U.S.C. § 401(x)(3)(B)(iv)) (prisoner data);
- Section 1611(e)(1)(I)(iii) of the Act (42 U.S.C. § 1382(e)(1)(I)(iii) (SSI);

- Section 205(r)(3) of the Act (42 U.S.C. § 405(r)(3)) and the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, § 7213(a)(2) (death data);
- Sections 402, 412, 421, and 435 of Pub. L. 104-193 (8 U.S.C. §§ 1612, 1622, 1631, and 1645) (quarters of coverage data);
- Children's Health Insurance Program Reauthorization Act of 2009, Pub. L. 111-3 (citizenship data); and
- Routine use exception to the Privacy Act, 5 U.S.C. § 552a(b)(3) (data necessary to administer other programs compatible with SSA programs).

This Agreement further carries out section 1106(a) of the Act (42 U.S.C. § 1306), the regulations promulgated pursuant to that section (20 C.F.R. Part 401), the Privacy Act of 1974 (5 U.S.C. § 552a), as amended by the CMPPA, related Office of Management and Budget (OMB) guidelines, the Federal Information Security Management Act of 2002 (FISMA) (44 U.S.C. § 3541, et seq.), and related National Institute of Standards and Technology (NIST) guidelines, which provide the requirements that the State must follow with regard to use, treatment, and safeguarding of data.

II. Scope

A. The State will ensure that State Agencies using SSA data to administer federally funded benefit programs will comply with the terms and conditions of this Agreement and the Privacy Act, as amended by the CMPPA. For the purpose of this Agreement, "State Agencies" do not include any tribal entities recognized by the U.S. Bureau of Indian Affairs.

B. Each State Agency that participates in data exchanges with SSA covered by this Agreement will execute one or more Information Exchange Agreements (IEA) with SSA, documenting additional terms and conditions applicable to those specific data exchanges, including the particular benefit programs administered by that State Agency, the data elements that will be disclosed, and the data protection requirements implemented to assist the State Agency in the administration of those programs.

C. The State, through its State Agencies, will use the SSA data governed by this Agreement to determine entitlement and eligibility of individuals for the following programs:

1. Temporary Assistance to Needy Families (TANF) program under Part A of title IV of the Act;
2. Medicaid provided under an approved State plan or an approved waiver under title XIX of the Act;

3. State Children's Health Insurance Program (CHIP) under title XXI of the Act, as amended by the Children's Health Insurance Program Reauthorization Act of 2009;
4. Supplemental Nutritional Assistance Program (SNAP) under the Food Stamp Act of 1977 (7 U.S.C. § 2011, et seq.);
5. Women, Infants and Children Program (WIC) under the Child Nutrition Act of 1966 (42 U.S.C. § 1771, et seq.);
6. Medicare Savings Programs (MSP) under 42 U.S.C. § 1396a(10)(E);
7. Unemployment Compensation programs provided under a state law described in section 3304 of the Internal Revenue Code of 1954;
8. Low Income Heating and Energy Assistance (LIHEAP or home energy grants) program under 42 U.S.C. § 8621;
9. State-administered supplementary payments of the type described in section 1616(a) of the Act;
10. Programs under a plan approved under titles I, X, XIV or XVI of the Act;
11. Foster Care and Adoption Assistance under title IV of the Act;
12. Child Support Enforcement programs under section 453 of the Act (42 U.S.C. § 653);
13. Other applicable federally funded programs administered by State Agencies under titles I, IV, X, XIV, XVI, XVIII, XIX, XX and XXI of the Act; and
14. Any other federally funded programs administered by State Agencies that are compatible with SSA's programs.

D. The State will ensure that SSA data disclosed for the specific purpose of administering a particular federally funded benefit program is used only to administer that program.

III. Justification and Expected Results

A. Justification

This Agreement and related data exchanges with State Agencies are necessary for SSA to assist the State in its administration of federally funded benefit programs by providing the data required to accurately determine entitlement and eligibility of individuals for benefits provided under these programs. SSA uses computer technology to transfer the data because it is more economical, efficient, and faster than using manual processes.

B. Expected Results

State Agencies will use the data provided by SSA to improve public service and program efficiency and integrity. The use of SSA data expedites the application process and ensures that benefits are awarded only to applicants that satisfy the State's program criteria. A cost-benefit analysis for the exchange made under this

Agreement is not required in accordance with the determination by the SSA Data Integrity Board (DIB) to waive such analysis pursuant to 5 U.S.C. § 552a(u)(4)(B).

IV. Record Description

A. Systems of Records

SSA SORs used for purposes of the subject data exchanges include:

- 60-0058 -- Master Files of SSN Holders and SSN Applications (accessible through EVS, SVES, or Quarters of Coverage Query data systems);
- 60-0059 -- Earnings Recording and Self-Employment Income System (accessible through BENDEX, SVES, or Quarters of Coverage Query data systems);
- 60-0090 -- Master Beneficiary Record (accessible through BENDEX or SVES data systems);
- 60-0103 -- Supplemental Security Income Record (SSR) and Special Veterans Benefits (SVB) (accessible through SDX or SVES data systems);
- 60-0269 -- Prisoner Update Processing System (PUPS) (accessible through SVES or Prisoner Query data systems).
- 60-0321 -- Medicare Part D and Part D Subsidy File

The State will ensure that the tax return data contained in **SOR 60-0059** (Earnings Recording and Self-Employment Income System) will only be used in accordance with 26 U.S.C. § 6103.

B. Data Elements

Data elements disclosed in computer matching governed by this Agreement are Personally Identifiable Information (PII) from specified SSA SORs, including names, SSNs, addresses, amounts, and other information related to SSA benefits, and earnings information. Specific listings of data elements are available at:

http://www.ssa.gov/gix/

C. Number of Records Involved

The number of records for each program covered under this Agreement is equal to the number of title II, title XVI, or title XVIII recipients resident in the State as recorded in SSA's Annual Statistical Supplement found on the Internet at:

http://www.ssa.gov/policy/docs/statcomps/

This number will fluctuate during the term of this Agreement, corresponding to the number of title II, title XVI, and title XVIII recipients added to, or deleted from, SSA databases during the term of this Agreement.

V. Notice and Opportunity to Contest Procedures

A. Notice to Applicants

State Agencies will notify all individuals who apply for federally funded, state-administered benefits under the Act that any data they provide are subject to verification through computer matching with SSA. State Agencies and SSA will provide such notice through appropriate language printed on application forms or separate handouts.

B. Notice to Beneficiaries/Recipients/Annuitants

State Agencies will provide notice to beneficiaries, recipients, and annuitants under the programs covered by this Agreement informing them of ongoing computer matching with SSA. SSA will provide such notice through publication in the Federal Register and periodic mailings to all beneficiaries, recipients, and annuitants describing SSA's matching activities.

C. Opportunity to Contest

State Agencies will not terminate, suspend, reduce, deny, or take other adverse action against an applicant for or recipient of federally funded, state-administered benefits based on data disclosed by SSA from its SORs until the individual is notified in writing of the potential adverse action and provided an opportunity to contest the planned action. "Adverse action" means any action that results in a termination, suspension, reduction, or final denial of eligibility, payment, or benefit. Such notices will:

1. Inform the individual of the match findings and the opportunity to contest these findings;

2. Give the individual until the expiration of any time period established for the relevant program by a statute or regulation for the individual to respond to the notice. If no such time period is established by a statute or regulation for the program, a 30-day period will be provided. The time period begins on the date on which notice is mailed or otherwise provided to the individual to respond; and

3. Clearly state that, unless the individual responds to the notice in the required time period, the State will conclude that the SSA data are correct and will

effectuate the threatened action or otherwise make the necessary adjustment to the individual's benefit or entitlement.

VI. Records Accuracy Assessment and Verification Procedures

State Agencies may use SSA's benefits data without independent verification. SSA has independently assessed the accuracy of its benefits data to be more than 99 percent accurate when they are created.

Prisoner and death data, some of which is not independently verified by SSA, does not have the same degree of accuracy as SSA's benefit data. Therefore, State Agencies must independently verify these data through applicable State verification procedures and the notice and opportunity to contest procedures specified in Section V of this Agreement before taking any adverse action against any individual.

SSA's citizenship data may be less than 50 percent current. Applicants for SSNs report their citizenship status at the time they apply for their SSNs. There is no obligation for an individual to report to SSA a change in his or her immigration status until he or she files a claim for benefits.

VII. Disposition and Records Retention of Matched Items

A. State Agencies receiving data from SSA to administer programs governed by this Agreement will retain all such data only for the required processing times for the applicable federally funded benefit programs and will then destroy all such data.

B. State Agencies may retain SSA data in hardcopy to meet evidentiary requirements, provided that they retire such data in accordance with applicable state laws governing State Agencies' retention of records.

C. State Agencies may use any accretions, deletions, or changes to the SSA data governed by this Agreement to update their master files of federally funded, state-administered benefit program applicants and recipients and retain such master files in accordance with applicable state laws governing State Agencies' retention of records.

D. State Agencies may not create separate files or records comprised solely of the data provided by SSA to administer programs governed by this Agreement.

E. SSA will delete electronic data input files received from State Agencies after it processes the applicable match. SSA will retire its data in accordance with the Federal Records Retention Schedule (44 U.S.C. § 3303a).

VIII. Security Procedures

The State will ensure that State Agencies using SSA data comply with the security and safeguarding requirements of the Privacy Act, as amended by the CMPPA, related OMB guidelines, FISMA, related NIST guidelines, and the current revision of IRS Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies and Entities*, available at http://www.irs.gov. In addition, State Agencies using SSA data will have in place administrative, technical, and physical safeguards for the matched data and results of such matches. Additional administrative, technical, and physical security requirements governing all data SSA provides electronically to State Agencies, including specific guidance on safeguarding and reporting responsibilities for PII, are set forth in the IEAs.

IX. Records Usage, Duplication, and Redisclosure Restrictions

A. State Agencies will use and access SSA data and the records created using that data only for the purpose of verifying eligibility for the specific federally funded benefit programs identified in the IEA.

B. State Agencies will comply with the following limitations on use, duplication, and redisclosure of SSA data:

1. State Agencies will not use or redisclose the data disclosed by SSA for any purpose other than to determine eligibility for, or the amount of, benefits under the state-administered income/health maintenance programs identified in this Agreement.

2. State Agencies will not use the data disclosed by SSA to extract information concerning individuals who are neither applicants for, nor recipients of, benefits under the state-administered income/health maintenance programs identified in this Agreement.

3. State Agencies will use the **Federal tax information (FTI)** disclosed by SSA only to determine individual eligibility for, or the amount of, assistance under a state plan pursuant to section 1137 programs and child support enforcement programs in accordance with 26 U.S.C. § 6103(l)(7) and (8). The State Agency receiving FTI will maintain all FTI from IRS in accordance with 26 U.S.C. § 6103(p)(4) and the IRS Publication 1075. Contractors and agents acting on behalf of the State Agency will only have access to tax return data where specifically authorized by 26 U.S.C. § 6103 and the current revision of IRS Publication 1075.

4. State Agencies will use the **citizenship status data** disclosed by SSA under the Children's Health Insurance Program Reauthorization Act of 2009, Pub. L. 111-3, only for the purpose of determining entitlement to Medicaid and CHIP programs for new applicants.

5. State Agencies will restrict access to the data disclosed by SSA to only those authorized State employees, contractors, and agents who need such data to perform their official duties in connection with the purposes identified in this Agreement.

6. State Agencies will enter into a written agreement with each of their contractors and agents who need SSA data to perform their official duties whereby such contractor or agent agrees to abide by all relevant Federal laws, restrictions on access, use, and disclosure, and security requirements in this Agreement. State Agencies will provide their contractors and agents with copies of this Agreement, related IEAs, and all related attachments before initial disclosure of SSA data to such contractors and agents. Prior to signing this Agreement, and thereafter at SSA's request, each State Agency will obtain from its contractors and agents a current list of the employees of such contractors and agents with access to SSA data and provide such lists to SSA.

7. State Agencies' employees, contractors, and agents who access, use, or disclose SSA data in a manner or purpose not authorized by this Agreement may be subject to civil and criminal sanctions pursuant to applicable Federal statutes.

C. State Agencies will not duplicate in a separate file or disseminate, without prior written permission from SSA, the data governed by this Agreement for any purpose other than to determine entitlement to, or eligibility for, federally funded benefits. A State Agency proposing the redisclosure must specify in writing to SSA what data are being disclosed, to whom, and the reasons that justify the redisclosure. SSA will not give permission for such redisclosure unless the redisclosure is required by law or essential to the conduct of the matching program and authorized under a routine use.

X. Comptroller General Access

The Comptroller General (the Government Accountability Office) may have access to all records of the State and its State Agencies that the Comptroller General deems necessary to monitor and verify compliance with this Agreement in accordance with 5 U.S.C. § 552a(o)(l)(K).

XI. Duration, Modification, and Termination of the Agreement

A. Duration

1. This Agreement is effective from July 1, 2012 (Effective Date) through December 31, 2013 (Expiration Date).

2. In accordance with the CMPPA, SSA will: (a) publish a Computer Matching Notice in the Federal Register at least 30 days prior to the Effective Date; (b) send required notices to the Congressional committees of jurisdiction under 5 U.S.C. § 552a(o)(2)(A)(i) at least 40 days prior to the Effective Date; and (c) send the required report to the OMB at least 40 days prior to the Effective Date.

3. Within 3 months prior the Expiration Date, the SSA DIB may, without additional review, renew this Agreement for a period not to exceed 12 months, pursuant to 5 U.S.C. § 552a(o)(2)(D), if:

   - the applicable data exchange will continue without any change; and
   - SSA and the State certify to the DIB in writing that the applicable data exchange has been conducted in compliance with this Agreement.

4. If either SSA or the State does not wish to renew this Agreement, it must notify the other party of its intent not to renew at least 3 months prior to the Expiration Date.

B. Modification

Any modification to this Agreement must be in writing, signed by both parties, and approved by the SSA DIB.

C. Termination

The parties may terminate this Agreement at any time upon mutual written consent of both parties. Either party may unilaterally terminate this Agreement upon 90 days advance written notice to the other party; such unilateral termination will be effective 90 days after the date of the notice, or at a later date specified in the notice.

SSA may immediately and unilaterally suspend the data flow or terminate this Agreement if SSA determines, in its sole discretion, that the State or a State Agency has violated or failed to comply with this Agreement.

XII. Reimbursement

In accordance with section 1106(b) of the Act, the Commissioner of SSA has determined not to charge the State and State Agencies the costs of furnishing the electronic data from the SSA SORs under this Agreement.

XIII. Disclaimer

SSA is not liable for any damages or loss resulting from errors in the data provided to State Agencies under any IEAs governed by this Agreement. Furthermore, SSA is not liable for any damages or loss resulting from the destruction of any materials or data provided by State Agencies.

XIV. Points of Contact

A. SSA Point of Contact

Regional Office

Brooks Hansen | Atlanta Data Exchange Coordinator
Center for Automation | Birmingham Information Technology Team
1200 Rev. Abraham Woods Jr. Blvd.
Birmingham, AL 35285
Phone: 205.801.1819/Fax: 205.801.1804
ATL.MOS.CA.DATA.EXCHANGE@ssa.gov

Heather Dawkins | Atlanta Data Exchange Coordinator
Center for Automation | Birmingham Information Technology Team
1200 Rev. Abraham Woods Jr. Blvd.
Birmingham, AL 35285
Phone: 205.801.1831/Fax: 205.801.1804
ATL.MOS.CA.DATA.EXCHANGE@ssa.gov

B. State Point of Contact

Bobby Waites
Chief Counsel to Governor Phil Bryant
Post Office Box 139
Jackson, Mississippi 39205
Phone: 601-576-2803/Fax: 601-359-3741
Bobby.waites@governor.ms.gov

SSA and Data Integrity Board Approval of Model CMPPA Agreement

The signatories below warrant and represent that they have the competent authority on behalf of SSA to approve the model of this CMPPA Agreement.

SOCIAL SECURITY ADMINISTRATION

Dawn S. Wiggins
Deputy Executive Director
Office of Privacy and Disclosure
Office of the General Counsel

1-17-2012
Date

I certify that the SSA Data Integrity Board approved the model of this CMPPA Agreement.

Daniel F. Callahan
Chair
SSA Data Integrity Board

1-26-2012
Date

XV. Authorized Signatures

The signatories below warrant and represent that they have the competent authority on behalf of their respective parties to enter into the obligations set forth in this Agreement. The State signatory below further acknowledges and agrees that, by his or her signature below, he or she represents State Agencies and is duly authorized to enter into the obligations set forth in this Agreement on behalf of those State Agencies.

SOCIAL SECURITY ADMINISTRATION

Michael W. Grochowski
Regional Commissioner
Atlanta Region

Date

MISSISSIPPI

Mississippi Governor Phil Bryant

4/2/12
Date

MISSISSIPPI DIVISION OF MEDICAID

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 PHI or PI 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 PHI or PI 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 PHI or PI. 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 PHI or PI, 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 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 encryption.*** DOM PHI and/or PI being processed or stored on any workstations and/or laptops must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as Advanced Encryption Standard (AES).

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

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

D. ***Removable media devices.*** All electronic files that contain DOM PHI or PI data must be encrypted when stored on any removable media or portable device (i.e. USB thumb drives, floppies, CD/DVD, Blackberry, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES.

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

F. ***Patch Management.*** All workstations, laptops and other systems that process and/or store DOM PHI or PI 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 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.

G. ***User IDs and Password Controls.*** All users must be issued a unique user name for accessing DOM PHI or PI. 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 24 hours. User IDs shall be locked out after 30 days of inactivity, disabled after 60 days of inactivity, and purged after 90 days of inactivity. Passwords are not to be shared. Passwords must be at least eight characters and must be a non-dictionary word. Passwords must not be stored in readable format on the computer. Passwords must be changed every 45 days, preferably every 30 days. Passwords must be changed if revealed or compromised. Passwords must be composed of characters from at least three of the following four groups from the standard keyboard:

- Upper case letters (A-Z)
- Lower case letters (a-z)
- Arabic numerals (0-9)
- Non-alphanumeric characters (punctuation symbols)

H. ***Data Destruction.*** When no longer needed, all DOM PHI or PI must be wiped using the Gutmann or US Department of Defense (DoD) 5220.22-M (7 Pass) standard, or by degaussing. Media may also be physically destroyed in accordance with NIST Special Publication 800-88. Other methods require prior written permission of DOM.

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

J. ***Warning Banners.*** All systems providing access to DOM PHI or PI 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.

K. ***System Logging.*** The system must maintain an automated audit trail which can identify the user or system process which initiates a request for DOM PHI or PI, or which alters DOM PHI or PI. 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 PHI or PI is stored in a database, database logging functionality must be enabled. Audit trail data must be archived for at least 3 years after occurrence.

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

M. ***Transmission encryption.*** All data transmissions of DOM PHI or PI outside the secure internal network must be encrypted using a FIPS 140-2 certified algorithm which is 128bit or higher, such as AES. Encryption can be end to end at the network level, or the data files containing PHI can be encrypted. This requirement pertains to any type of PHI or PI in motion such as website access, file transfer, and E-Mail.

N. ***Intrusion Detection.*** All systems involved in accessing, holding, transporting, and protecting DOM PHI or PI 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 PHI or PI 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.

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

C. ***Change Control.*** All systems processing and/or storing DOM PHI or PI 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 PHI or PI 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 24 hours.

B. ***Data Backup Plan.*** User must have established documented procedures to backup DOM PHI to maintain retrievable exact copies of DOM PHI or PI. 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 PHI or PI 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 PI 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 PI 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 PI is contained shall be escorted and DOM PHI or PI shall be kept out of sight while visitors are in the area.

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

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

E. ***Faxing.*** Faxes containing DOM PHI or PI 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 PHI or PI shall be sealed and secured from damage or inappropriate viewing of PHI or PI to the extent possible. Mailings which include 500 or more individually identifiable records of DOM PHI or PI 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.

MISSISSIPPI DIVISION OF MEDICAID

DATA USE AGREEMENT

Attachment D

Notification of Breach

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

II. **Breaches and Security Incidents.** During the term of this Agreement, User agrees to implement reasonable systems for the discovery and prompt reporting of any Breach or security incident, and 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 a Breach of unsecured PHI or PI in electronic media or in any other media if the PHI or PI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, or upon the discovery of a suspected security incident that involves data provided to DOM by the Social Security Administration. (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 suspected security incident, intrusion or unauthorized access, Use or Disclosure of PHI or PI in Violation of this Agreement and this Attachment, or potential loss of confidential data affecting this Agreement. A Breach shall be treated as discovered by User as of the first day on which the Breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the Breach) 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 is reasonably believed by User 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 42 U.S.C. § 17932 and 45 C.F.R. Parts 160 and 164, Subparts A, D, and E.

Upon discovery of a Breach or suspected security incident, intrusion or unauthorized access, Use or Disclosure of PHI or PI, User shall take:

a. Prompt corrective action to mitigate any risks or damages involved with the Breach and to protect the operating environment; and

b. Any action pertaining to such unauthorized Disclosure required by applicable Federal and State laws and regulations.

B. ***Investigation and Investigation Report.*** To immediately investigate such security incident, Breach, or unauthorized access, Use or Disclosure of PHI or PI, 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 the Breach or unauthorized Use or Disclosure. The report shall include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper Use or Disclosure. 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 a Breach of PHI or PI is attributable to User or its Subcontractors, agents or vendors, User shall notify Individuals of the Breach or unauthorized Use or Disclosure 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. 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 in subsection 1, above.

III. ***Contact Information.*** To direct communications to the above referenced staff, the 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 the User. Said changes shall not require an amendment to this Attachment or the Data Use Agreement to which it is incorporated.

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

DOM Security Officer:	Address:	550 High Street, Suite 1000, Jackson, MS 39201
	Telephone:	(601) 359-6050
DOM Privacy Officer:	Address:	550 High Street, Suite 1000, Jackson, MS 39201
	Email:	privacyofficer@medicaid.ms.gov
	Telephone:	(601) 359-6118
	Fax:	(601) 359-9620

MISSISSIPPI DIVISION OF MEDICAID

DATA USE AGREEMENT

Attachment E

Certificate of Return or Destruction of Confidential Data

I, _____ (name of Custodian of the File(s)), hereby certify the following to be true and correct:

I. I am employed by _____ (name of User(s)) as a(n) _____ (occupation).

II. Pursuant to the attached Data Use Agreement ("Agreement") between the Mississippi Division of Medicaid ("DOM") and _____ (name of User(s)), I received and acted as custodian of the data described in Attachment A of the Agreement.

III. ☐ The purpose for receiving some of the data described in Attachment A has been met.

OR

☐ The purpose for receiving some of the 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 data indicated in section (III) of this Certificate of Return or Destruction of Confidential Data has been returned to DOM by _____ (method of return) or destroyed by _____ (method of destruction) on _____ (date of return/destruction).

_____ _____
(Signature of Custodian of the File(s)) (Date)

MEMORANDUM OF UNDERSTANDING
BETWEENTHE
DIVISION OF MEDICAID IN THE OFFICE OF THE GOVERNOR
STATE OF MISSISSIPPI
AND THE
MISSISSIPPI STATE DEPARTMENT OF HEALTH
(Maternal and Infant Vital Records Data)

THIS MOU made and entered into by and among the **Division of Medicaid in the Office of the Governor,** an administrative agency of the State of Mississippi, hereinafter referred to as "DOM," and the **Mississippi State Department of Health,** an administrative agency of the State of Mississippi, hereinafter referred to as "MSDH." The Parties have prepared this Memorandum of Understanding ("MOU") to establish, support, and promote a collaborative effort to coordinate maternal and infant vital records data for research purposes.

WHEREAS, DOM maintains claims data related to maternal and infant beneficiaries;

WHEREAS, MSDH maintains vital records for Mississippi citizens, including mothers and infants in Mississippi.

WHEREAS, studies have suggested the linkage of claims data and vital records statistics can help guide initiatives to improve birth outcomes and care for mothers and infants receiving Medicaid, as well as provide performance monitoring and quality control measures.

WHEREAS, DOM and MSDH are significant segments of Mississippi's public health infrastructure.

WHEREAS, the parties desire to set forth in this MOU, which is not legally binding, plans to work together to place focus on and/or achieve the principles, goals and objectives described herein.

NOW THEREFORE, in furtherance of this alliance, the parties agree as follows:

I. OBJECTIVES

A. Work together to link Medicaid claims data and MSDH vital records data for mothers and infants for the purpose of research.

B. Whenever possible, craft a method for linking data that will, once data is linked, remove personal identifiers.

C. Analyze the data for the purpose of guide initiatives to improve birth outcomes and care for mothers and infants receiving Medicaid, as well as provide performance monitoring and quality control measures.

D. Participate in joint training efforts related to data linkage, including training provided by the Centers for Disease Control and Prevention and the Center for Medicare & Medicaid Services.

II. **PERIOD OF PERFORMANCE:** The term of this MOU shall commence on February 15, 2014, and shall remain in force through February 1, 2018, unless terminated earlier by any party upon thirty (30) days written notice to the other parties.

III. **COORDINATION AND COOPERATION:** The Parties will support cooperation in the provision of the above-noted programs to support the specific goals of the alliance in accordance with the provisions of this MOU, with Mississippi and federal law, and the regulations of all applicable organizations. Each Party intends to utilize reasonable efforts to implement this MOU, and each part commits to appoint representative members to a collective committee to move forward with consideration of the issues herein described.

IV. **RELATIONSHIP OF PARTIES:** It is expressly understood and agreed that this MOU is in no way based on an employer-employee relationship.

V. **NON-ASSIGNMENT AND SUBCONTRACTING:** Each Party understands that it will not assign this MOU to any other person or entity.

VI. **MODIFICATION OR AMENDMENT:** Modifications or amendments to this MOU may be made upon mutual agreement of the Parties, in writing signed by the Parties hereto and approved as required by law.

VII. **TERMINATION:** Any party may terminate this MOU at any time, with or without cause, by giving written notice to the other parties of such termination and specifying the effective date thereof, at least thirty (30) days before the effective date of such termination. No party will be liable to any other party for termination of this MOU.

XI. **AVAILABILITY OF FUNDS:** To the extent funding is applicable, it is expressly understood and agreed that the obligation of all parties to proceed under this MOU is conditioned upon the appropriation of funds by the Mississippi State Legislature and the receipt of federal and/or state funds for the operation of each party.

XII. **SEVERABILITY:** It is understood and agreed by the parties hereto that if any part, term or provision of this MOU 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 MOU did not contain that particular part, term, or provision held to be invalid.

XIII. **CONFIDENTIALITY:** The parties agree that they shall not use or disclose for any purpose other than those described herein any information concerning any beneficiary or provider of services that it may have access to or have knowledge of as a result of this MOU. However, the obligation of confidentiality shall not apply to information that is required to be disclosed pursuant to law or the legal process. This confidentiality

agreement survives the term of the MOU. The parties expressly agree to execute a Business Associate Agreement and/or Data Use Agreement whenever one party deems such document necessary.

XIV. **APPLICABLE LAW:** This MOU shall be governed by and construed in accordance with the laws of the State of Mississippi, excluding its conflicts of laws provisions. The parties shall comply with applicable federal, state and local laws, regulations, policies and procedures as now existing and as may be amended or modified.

XV. **NON-DISCRIMINATION:** In connection with the performance and obligations of work under this MOU, the parties are all equal opportunity employers and therefore, maintain a policy which prohibits unlawful discrimination based on race, color, creed, religion, sex, age, national origin, physical handicap, disability, genetic information, political affiliation, ancestry, limited English proficiency, or any other consideration made unlawful by federal, State, or local laws. All such discrimination is unlawful and the parties agree that they will strictly adhere to this policy in their employment practices and provision of services, including, but not limited to, hiring, termination/discharge, promotion/demotion, or other terms and conditions of employment.

XIX. **INDEMNIFICATION:** As governmental entities, the parties' tort obligations are set forth in the Mississippi Tort Claims Act.

XX. **THIRD PARTY ACTION NOTIFICATION:** The parties shall give each other prompt notice in writing of any action or suit filed, and prompt notice of any claim made against any party that may result in litigation related in any way to this MOU.

XXI. **NOTICES:** Any notice from one party to the other under this MOU shall be in writing and shall be sent to the other party by U.S. Mail, postage prepaid, at its principal business address, unless changed by either party hereto by written notice similarly given.

XXII. **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996:** All activities under this MOU shall be performed in accordance with all applicable federal and/or state laws, rules and/or regulations including the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A, and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, and their implementing regulations at 45 C.F.R. Parts 160, 162, and 164, involving electronic data interchange, code sets, identifiers, and the security and privacy of protected health information, as may be applicable to the services under this MOU. Each party to this MOU shall treat all data and information to which it has access under this MOU as confidential information to the extent that confidential treatment of same is required under federal and state law and shall not disclose same to a third party without specific written consent of the other party. In the event that either party receives notice that a third party requested divulgence of the confidential or otherwise protected information and/or has served upon it a subpoena or other validly issued administrative or judicial process ordering divulgence of the

confidential or otherwise protected information, the party shall promptly inform the other party and thereafter respond in conformity with such subpoena as required by applicable state and/or federal law, rules, and regulations. The provision herein shall survive the termination of the MOU for any reason and shall continue in full force and effect and shall be binding upon all parties and their agents, employees, successors, assigns, subcontractors, or any party claiming an interest in the MOU on behalf of, or under, the rights of the parties following termination.

XXIII. INSPECTIONS: All parties agree that representatives of the Comptroller General, CMS, the General Accounting Office, the State Auditor, DOM and their authorized representatives shall have the right during regular business hours to inspect and copy MCHS's books and records pertaining to the work performed under this MOU. The parties shall cooperate fully with the request from any of the agencies listed above and shall furnish free of charge copies of all requested records.

XXIV. RECORDS RETENTION AND AUDIT PROCEDURES: MSDH shall maintain financial records, supporting documents, statistical reports, and all other records pertinent to this program for a period of five (5) years from the termination or expiration of this MOU. However, if audit, litigation, or other legal action by or on behalf of the State or Federal Government has begun that is not completed at the end of the five (5) year period, or if audit findings, litigation, or other legal action has not been resolved at the end of the five (5) year period, the records shall be retained until resolution.

XXV. OTHER PROVISIONS: If applicable, the parties agree to all of the provisions and requirements as set forth in the State Plan for Medical Assistance approved by the State of Mississippi and by the Secretary of the United States Department of Health and Human Services, pursuant to Title XIX of the Social Security Act, and understands those provisions and requirements are also incumbent on the MSDH.

XXVI. COMPLIANCE WITH MISSISSIPPI EMPLOYMENT PROTECTION ACT (MEPA): The parties represent and warrant that they will ensure its compliance with the Mississippi Employment Protection Act, Section 71-11-1 et seq. of the Mississippi Code Annotated (Supp. 2008), and will register and participate in the status verification system for all newly hired employees. The term "employee" as used herein means any person that is hired to perform work within the State of Mississippi. As used herein, "status verification system" means the Illegal Immigration Reform and Immigration Responsibility Act of 1996 that is operated by the United States Department of Homeland Security, also known as the E-Verify Program, or any other successor electronic verification system replacing the E-Verify Program. MSDH agrees to maintain records of such compliance and, upon request of the State and approval of the Social Security Administration or Department of Homeland Security, where required, to provide a copy of each such verification to the State. MSDH further represents and warrants that any person assigned to perform services hereunder meets the employment eligibility requirements of all immigration laws of the State of Mississippi. MSDH understands and agrees that any breach of these warranties may subject MSDH to the following: (a) termination of this MOU and ineligibility for any state or public contract in Mississippi for up to three (3) years, with notice of such cancellation/termination being made public,

or (b) the loss of any license, permit, certification or other document granted to MSDH by an agency, department or governmental entity for the right to do business in Mississippi for up to one (1) year, or (c) both. In the event of such termination/cancellation, MCHS would also be liable for any additional costs incurred by the State due to contract cancellation or loss of license or permit.

XXVII. **REPRESENTATION REGARDING CONTINGENT FEES:** If applicable, the parties represent that they have not retained a person to solicit or secure this MOU upon an agreement or understanding for a commission, percentage, brokerage, or contingent fee.

XXVIII. **REPRESENTATION REGARDING GRATUITIES:** The parties agree that they have not violated, is not violating, and promises that it will not violate the prohibition against gratuities set forth in Section 6-204 (Gratuities) of the Mississippi Personal Service Contract Rules and Regulations.

XXIX. **TRANSPARENCY MISSISSIPPI:** In accordance with the Mississippi Accountability and Transparency Act of 2008, Section 27-104-151, et seq., of the Mississippi Code of 1972, as amended, the American Accountability and Transparency Act of 2009 (P.L. 111-5), where applicable, and Section 31-7-13 of the Mississippi Code of 1972, as amended, where applicable, a fully executed copy of this MOU shall be posted to the State's accountability website at: https://www.transparency.mississippi.gov.

XXX. **OWNERSHIP AND FINANCIAL DISCLOSURE:**

A. In accordance with 42 C.F.R. § 455.104(b), MSDH and UMMC (for purposes of this paragraph, "Contractor") shall disclose the following:

1. The name and address of any person (individual or corporation) with an ownership or control interest in the disclosing entity, DOM's fiscal agent, or managed care entity. The address for corporate entities must include as applicable primary business, every business location, and P.O. Box address;

2. Date of birth and Social Security Number (in the case of an individual);

3. Other tax identification number (in the case of a corporation) with an ownership or control interest in the disclosing entity (or DOM's fiscal agent or managed care entity) or in any subcontractor in which the disclosing entity (or DOM's fiscal agent or managed care entity) has a 5 percent or more interest;

4. Whether the person (individual or corporation) with any ownership or control interest in the disclosing entity (or DOM's fiscal agent or managed care entity) is related to another person with ownership

or control interest in the disclosing entity as a spouse, parent, child, or sibling; or whether the person (individual or corporation) with an ownership or control interest in any subcontractor in which the disclosing entity (or DOM's fiscal agent or managed care entity) has a 5 percent or more interest is related to another person with ownership or control interest in the disclosing entity as a spouse, parent, child, or sibling;

5. The name of any other disclosing entity (or DOM's fiscal agent or managed care entity) in which an owner of the disclosing entity (or DOM's fiscal agent or managed care entity) has an ownership or control interest; and,

6. The name, address, date of birth, and Social Security Number of any managing employee of the disclosing entity (or DOM's fiscal agent or managed care entity).

B. In accordance with 42 C.F.R. § 455.104(c), disclosures from the Contractor are due at any of the following times:

1. Upon the Contractor submitting a proposal in accordance with the State's procurement process;

2. Annually, including upon the execution, renewal, and extension of the contract with the State; and,

3. Within 35 days after any change in ownership of the Contractor.

C. In accordance with 42 C.F.R. § 455.104(d), all disclosures must be provided to DOM, the State's designated Medicaid agency.

D. In accordance with 42 C.F.R. § 455.104(e), federal financial participation (FFP) is not available in payments made to a disclosing entity that fails to disclose ownership or control information as required by said section.

E. In accordance with 42 C.F.R. § 455.105, the Contractor must fully disclose all information related to business transactions. The Contractor must submit, within 35 days of the date on a request by the Secretary or DOM, full and complete information about:

1. The ownership of any subcontractor with whom the Contractor has had business transactions totaling more than $25,000 during the 12-month period ending on the date of the request; and,

2. Any significant business transactions between the Contractor and any wholly owned supplier, or between the Contractor and any subcontractor, during the 5-year period ending on the date of the request.

F. In accordance with 42 C.F.R. § 455.106(a), the Contractor must disclose to DOM the identity of any person who:

1. Has ownership or control interest in the Contractor, or is an agent or managing employee of the Contractor; and,

2. Has been convicted of a criminal offense related to that person's involvement in any program under Medicare, Medicaid, or the Title XX services program since the inception of those programs.

G. In accordance with 42 C.F.R. § 455.106(b), DOM must notify the Inspector General of the Department of any disclosures under § 455.106(a) within 20 working days from the date it receives the information. DOM must also promptly notify the Inspector General of the Department of any action it takes on the Contractor's MOU and participation in the program.

H. In accordance with 42 C.F.R. § 455.106(c), DOM may refuse to enter into or renew an MOU with a Contractor if any person who has an ownership or control interest in the Contractor, or who is an agent or managing employee of the Contractor, has been convicted of a criminal offense related to that person's involvement in any program established under Medicare, Medicaid or the Title XX Services Program. Further, DOM may refuse to enter into or may terminate a Contractor MOU if it determines that the Contractor did not fully and accurately make any disclosure required under 42 C.F.R. § 455.106(a).

I. In accordance with 42 C.F.R. § 455.436, the State Medicaid agency and all Medicaid contractors shall do the following:

1. Confirm the identity and determine the exclusion status of contractors/subcontractors and any person with an ownership or control interest or who is an agent or managing employee of the contractor/subcontractor through routine checks of federal databases; and,

2. Consult appropriate databases to confirm identity of the above-mentioned persons and entities by searching the List of Excluded Individuals/Entities (LEIE) and the System for Award Management (SAM) upon enrollment, re-enrollment, credentialing, or re-credentialing, and no less frequently than monthly thereafter, to ensure that the State does not pay federal funds to excluded persons or entities.

IN WITNESS WHEREOF, the parties have executed this MOU to be effective as of the 1 day of Feb, 2014.

FOR DIVISION:

DIVISION OF MEDICAID
IN THE OFFICE OF THE GOVERNOR
STATE OF MISSISSIPPI

BY: _____
David J. Dzielak, Ph.D.
EXECUTIVE DIRECTOR

FOR MISSISSIPPI STATE DEPARTMENT OF HEALTH

BY: _____
Mary Currier, MD, MPH
STATE HEALTH OFFICER

STATE OF MISSISSIPPI
COUNTY OF Hinds.

THIS DAY personally came and appeared before me, the undersigned authority, in and for the aforesaid jurisdiction, the within named, **David J. Dzielak, Ph.D.,** in his official capacity as the duly appointed **Executive Director of the Division of Medicaid in the Office of the Governor,** an administrative agency of the State of Mississippi, who acknowledged to me, being first duly authorized by said agency that he signed and delivered the above and foregoing written Contractual MOU for Professional Services for and on behalf of said agency, and as its official act and deed on the day and year therein mentioned.

GIVEN under my hand and official seal of office on this the 13th day of May, A.D., 2014.

_____
NOTARY PUBLIC

MY COMMISSION EXPIRES:

STATE OF MISSISSIPPI
SARAH O. SMITH
ID No
69424
NOTARY PUBLIC
Comm Expires
April 7, 2015
RANKIN COUNTY

STATE OF MISSISSIPPI
COUNTY OF Hinds

THIS DAY personally came and appeared before me, the undersigned authority, in and for the aforesaid jurisdiction, the within named, **Mary Currier, MD, MPH,** in his official capacity as the duly appointed **State Health Officer, Mississippi State Department of Health,** who acknowledged to me, being first duly authorized by said corporation that he signed and delivered the above and foregoing written MOU for and on behalf of said corporation, and as its official act and deed on the day and year therein mentioned.

GIVEN under my hand and official seal of office on this the 29th day of April, A.D., 2014.

Gwen Wood Black
NOTARY PUBLIC

STATE OF MISSISSIPPI NOTARY PUBLIC ID # 47341 GWEN WOOD BLACK Commission Expires Oct. 27, 2016 RANKIN COUNTY

MY COMMISSION EXPIRES: _____

Attachment F

Dear Mississippi State Colleagues,

On behalf of the Centers for Disease Control and Prevention (CDC) and Center for Medicare & Medicaid Services (CMS), I'm writing to invite Mississippi to participate in a ten-month project designed to assist selected states in linking Medicaid claims and Vital Statistics data for surveillance, performance monitoring, and quality improvement purposes. Our understanding is that your state may benefit from assistance with linking datasets, whether it is obtaining data use agreements or performing the actual linkages. If this is the case, we hope you and your state colleagues will take this opportunity to participate in trainings with expert faculty and experienced state peers.

The ten-month project begins in December 2013 and entails an in-person training in late January/early February 2014, as well as monthly Web trainings. The goal of the trainings will be to improve measurement of various maternal and child health indicators, especially the two measures in the CMS Core Set of Children's Health Care Quality Measures for Medicaid and CHIP that require data linkage (C-section and low birth weight rates). AcademyHealth is contracted to manage this project with the CDC Project Officer, Dr. Danielle Barradas.

We do hope your state can build a team with representation from Medicaid, Vital Statistics, SSDI, and Title V to participate in the monthly trainings, as successful data linkages of this nature require collaboration across state offices. However, we can only support travel of one data analyst to attend the in-person, overnight training.

Please coordinate between the departments and let us know if your state is interested in participating in the project by **Thursday, December 5, 2013.** While the Web trainings are open to all relevant state staff, please complete the attached form with contact information for two state project leads, 1) the analyst that will perform the linkage and participate in the in-person training and 2) a member of the state Medicaid agency that can join monthly Web trainings and assist in measure collection. We will then be in touch to schedule the monthly Web trainings and confirm that date of the in-person meeting.

We should also note that CMS is supporting more intensive linkage technical assistance to some of the states with Strong Start grants that do not already do data linkages. While we are on a different timeline (they will be contacting states in a few months), we are coordinating project activities so you can participate in both if invited.

For additional information or to confirm your participation, please feel free to contact me at Katherine.Griffith@academyhealth.org or 202.292.6730.

We look forward to hearing from and hopefully working with you soon!

Thank you for your consideration,

Katherine Griffith

Attachment F

Linking Medicaid Data to Vital Records to Better Understand Birth Outcomes in Mississippi

Charlene H. Collier MD, MPH, MHS

Background: Over sixty percent of the births in Mississippi are covered by Medicaid, demonstrating the large proportions of births occurring to low-income women in Mississippi. Despite recent improvements, Mississippi continues to have among the highest rates of several poor birth outcomes including prematurity, low birth weight, infant mortality and maternal death. On a population level, vital records including birth and death certificates are the most common data sources used to evaluate birth outcomes. However, birth certificates lack information on treatments women receive, specific diagnosis, frequency and duration of hospital encounters and costs. Medicaid enrollment and claims data contain a wealth of information related to pregnancy management and health conditions during pregnancy that is lacking in birth certificate data. In linking birth certificate data with Medicaid data the resulting data provide a more complete picture for evaluating services and outcomes for pregnancies.

Purpose: There are a number of in-depth analysis regarding pregnancy care and birth outcomes that can be accomplished with linked Medicaid and birth certificate data. First, birth outcomes within the Medicaid population can be evaluated and compared to the privately insured population. As birth certificate data is linked to infant death records, adding Medicaid data provides an enhanced picture of maternal comorbid conditions, intrapartum diagnosis and procedures received during care that may affect infant outcomes. The quality of care received by women on Medicaid can be assessed by identifying the number of prenatal visits, cesarean delivery rates, complications, Emergency Department visits, readmissions and prolonged hospitalizations. There are particular medical practices, including non-medically indicated cesareans and inductions which are known to contribute to higher costs and worse outcomes. Linked data would allow a more accurate assessment of elective early deliveries in Mississippi and if they are associated with poor outcomes. Alternatively, the use of high quality treatments including progesterone therapy to prevent preterm birth or effective contraceptive care in the post partum period can also be assessed.

Methods: Data will be obtained from vital statistics data from the Vital Records Office of the Department of Health and Medicaid claims data from the Mississippi Division of Medicaid. Data sharing policies and agreements will be agreed upon prior to data sharing. Data will be,linked using a multi-step approach matching unique identifiers including first and last name, address, date of birth and delivery date. Once linked, the personal identifiers will be removed from the data set and replaced with a study identification number. The data will be analyzed for frequency statistics and analytic comparisons will be made between publicly insured and privately insured and other demographic groups. Associations between patient characteristics and outcomes will be analyzed.

Implications: This data can help guide initiatives to improve birth outcomes and improve care for pregnant women who receive Medicaid. Given the large percentage of births financed by Medicaid, this analysis will provide meaningful insight into the birth experiences of women in Mississippi.

Attachment F

Additional Codes of Interest

- ICD-9-CM Codes:
  - 73.01 Induction of labor by artificial rupture of membranes
  - 73.1 Other surgical induction of labor
  - 73.4 Medical induction of labor
- Cesarean section as defined by the following ICD-9-CM codes while not in Active Labor[1] or experiencing Spontaneous Rupture of Membranes[2]:
  - 74.0 Classical cesarean section
  - 74.1 Low cervical cesarean section
  - 74.2 Extraperitoneal cesarean section
  - 74.4 Cesarean section of other specified type
  - 74.99 Other cesarean section of unspecified type
- Prenatal Care
  - Supervision of normal pregnancy
    - V22.0 – V22.
  - Supervision of high risk pregnancy
    - V23
- Postpartum care
  - V24.0 – V24.2