No. _____
[Document number assigned by Medicaid Legal Division]

DATA SHARING AGREEMENT
BETWEEN

_____
AND
THE ALABAMA MEDICAID AGENCY

I. Purpose.

The purpose of this agreement is to address the security requirements that must be met and to establish the terms and conditions under which the _____ (hereinafter referred to as _____) will obtain access to data maintained by the Alabama Medicaid Agency (hereinafter referred to as "Medicaid").

This agreement may not be assigned nor delegated without prior approval by the Commissioner of Medicaid or as documented in this agreement. _____ agrees that it is responsible for compliance with the terms of this agreement for all employees, subcontractors or agents and must obtain a fully executed agreement to be bound by these restrictions from each subcontractor or agent prior to receiving information from Medicaid. Furthermore, any data shared with employees, subcontractors or agents will be subject to all applicable requirements regarding privacy and confidentiality that are described herein.

II. Background.

The widespread growth in communications has significantly enhanced the opportunity to use advanced information technology for interaction and data sharing among public and private sectors. However, the advantages provided by such technology come with an element of risk to the confidentiality and integrity of data. Below is a background on why data covered under this agreement is to be shared between _____ and Medicaid.

The state of Alabama is soliciting responses for Request for Proposal (RFP) 2019-ACHN-01 in an effort to implement a consolidated Care Coordination system to address issues with the health status of Medicaid Eligible Individuals (EIs) and the level of quality of existing services.

To achieve this objective, Medicaid is making available a limited data set to potential proposers to enable an accurate and efficient price proposal response to the RFP.

III. Effective Date.

This agreement shall take effect as of the date of signature by both parties.

IV. Expiration Date.

This agreement shall remain in effect until superseded or canceled. In the event of cancellation, written notice of such termination must be provided by the canceling party;

in which case, the termination shall be effective 30 days after the date of the notice or at a later date specified in the termination notice.

In the event of a violation of the terms specified herein, Medicaid has the right to immediately terminate this agreement.

V. Definitions.

1. Integrity:
   The ability to protect information against the threat of modification by unauthorized users. This includes the ability to certify that information or data was not modified or was legitimately modified during communication or in storage.

2. Access Control:
   The ability for users and operators to precisely control who accesses which resources. This also includes control of what level of access is allowed.

3. Authentication:
   The process of verifying an identity or credential, to ensure you are who you say you are and the message has not been altered in transit.

4. Nonrepudiation or Accountability:
   The ability to prevent communicating parties in the network from denying that they sent or received given messages or engaged in particular network activities.

5. Confidentiality:
   The ability to restrict access to authorized users only and protect information against the threat of disclosure to or theft by unauthorized users.

6. Privacy:
   The ability to ensure that personal and unrelated information are not unnecessarily disclosed.

VI. Amendments.

Any amendments to this agreement must be in writing and signed by both parties.

VII. Policy.

This agreement establishes the fundamental rules and requirements for the exchange of sensitive Medicaid information with _____ and sets forth the terms under which _____ agrees to furnish data to Medicaid and receive data from Medicaid.

It is permissible to use electronic media for transmission as long as an acceptable method is utilized to provide for confidentiality and integrity of this data, and that

authentication or identification procedures are employed to assure that both the sender and recipient of the data are known to each other and are authorized to receive and use such information.

VIII. Confidentiality.

_____ agrees to establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use or access to it in accordance with 42 C.F.R. 431.300 et seq. Any results of the data exchange, which contains individually identifiable data, cannot be released outside your agency unless agreed to by Medicaid.

_____ represents and warrants further that, except as specified in this document or except as authorized in writing, it will not disclose, release, reveal, show, sell, rent, lease, loan or otherwise grant access to Medicaid data to any person. Access to the data covered by this agreement shall be limited to the minimum number of individuals necessary to achieve the purpose stated in this agreement and to those individuals on a need-to-know basis only.

_____ shall not permit access to Medicaid data for third parties, nor assign or delegate duties described herein to third parties without the prior written agreement of Medicaid. All third parties are prohibited from the independent use of information, statistics, project results, and reports prepared pursuant to this agreement without the prior written approval of the Commissioner of Medicaid. All proposed publications of any kind that use the data generated by this exchange of information must receive prior written approval of the Commissioner of Medicaid before they are published. _____ understands that any damages arising out of the unauthorized and misuse of this data on your behalf will be the responsibility of _____.

Any disclosure of information must be approved in advance by the Commissioner of Medicaid and then only to individuals expressly authorized to review such information under federal or state laws. If _____, employees, subcontractors or agents, discloses or attempts to disclose confidential information it is understood that an injunction may be obtained to prevent that disclosure as well as any other remedies at law that may be available.

When deemed necessary by Medicaid, all confidential information must be returned to Medicaid upon written request.

IX. Security Controls.

1. Media Controls.
   In the event that data is exchanged via diskettes, compact disc (CD), tapes, File Transfer Protocol (FTP) etc., Medicaid requires that formal, documented procedures govern the receipt and removal of such media into and out of a facility to ensure total control of Medicaid information.

In the event that data is exchanged via the Internet or FTP adequate encryption and the employment of authentication/identification techniques are required for use in safeguarding sensitive Medicaid information. Furthermore, Medicaid reserves the right to audit any organization's implementation of, and/or adherence to the requirements, as stated in this agreement upon thirty (30) day notice during reasonable business hours. This includes the right to require that any organization utilizing the Internet or FTP for transmission of Medicaid sensitive information submit documentation to demonstrate that it meet the requirements contained in this agreement.

2. Physical Access Controls.
   Physical access control (limited access) is required. Medicaid requires procedures for limiting physical access to Medicaid information by ensuring that only authorized personnel have proper access.

3. Workstation Controls.
   Each organization is required to have a policy/guideline on workstation use. These documented instructions/procedures must delineate the proper functions to be performed and the manner in which those functions are to be performed (for example, logging off before leaving a workstation unattended). This is important so that employees understand the manner in which workstations must be used to maximize the security of recipient information.

4. Workstation Location.
   Each organization is required to put in place physical safeguards to eliminate or minimize the possibility of unauthorized access to information due to the location of a workstation.

X. Justification for Access.

The state of Alabama is soliciting responses for Request for Proposal (RFP) 2019-ACHN-01 in an effort to implement a consolidated Care Coordination system to address issues with the health status of Medicaid Eligible Individuals (EIs) and the level of quality of existing services.

To achieve this objective, Medicaid is making available a limited data set to potential proposers to enable an accurate and efficient price proposal response to the RFP.

XI. Description of Data.

"Data" possibly could mean adjudicated claims data on Alabama health care provider, summary of medical claims for children and adults together with eligibility data that includes each month of eligibility per member, region/county information, zip code, gender, and age for Fiscal Years 2014 - 2016. The data is restricted to exclude name, address, SSN, and Medicaid ID.

The data will not contain actual Medicaid identification numbers or social security numbers, but will be linked through a unique identification number that Medicaid will be able to trace back to the initial recipient. While addresses for billing providers will be provided, geographic information on the recipients will be limited to zip codes.

_____ Technical contacts for Data Format and Content

Contact Name & Title	Contact Information	Contact for Questions Regarding:

Medicaid Technical contacts for Data Format and Content

Contact Name & Title	Contact Information	Contact for Questions Regarding:
Drew Nelson, MPH Quality Assurance	Drew.nelson@medicaid.alabama.gov Phone: 334-353-3216	Data content, format, and submission
Michael E. Kelley, Director Application Development and Support	334-353-4106 Michael.Kelley@Medicaid.Alabama.gov	Data content, format, and submission

XII. Method of Data Access or Transfer.

Data will be transferred utilizing appropriate administrative, physical, and technical safeguards that are compliant with the standards set forth in the HIPAA Security Rule (i.e. secure FTP or encrypted hard drive). These security measures will be such that the integrity of the data is maintained and the risk of unauthorized use or disclosure is minimized to the extent reasonably possible.

_____ Email Notification List

Email Contact Name & Title	Contact Information

Medicaid Email Notification List

Email Contact Name & Title	Contact Information
Michael Kelley, Director IT Application Development & Support	Michael.kelley@medicaid.alabama.gov 334-353-4106
Barry Cambron, MBA Quality Analytics	Barry.Cambron@medicaid.alabama.gov Phone: 334-353-4214

XIII. Data Sharing Financial Obligations.

The Parties do not anticipate that there will be costs incurred in connection with the production of data shared under this agreement. However, to the extent that costs are incurred, each Party here under shall be responsible for its own costs associated thereto.

XIV. Data Breaches.

_____ shall notify Medicaid no later than one (1) business day following the discovery of a breach of Protected Health Information (PHI).

_____ shall provide the following information and obtain Medicaid approval prior to reporting a breach required by 45 C.F.R. Part 164, Subpart D:

- The number of records involved in the breach.
- A brief description of what happened, including the date of the breach and the date of the discovery of the breach if known.
- A description of the types of unsecure protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other type information were involved).
- Any steps the individuals should take to protect themselves from potential harm resulting from the breach.
- A brief description of what _____ is doing to investigate the breach, to mitigate harm to individuals and to protect against any further breaches.
- Contact procedures for individuals to ask questions or learn additional information, which shall include _____ toll-free number or direct number, email address, Web site, or postal address.
- A proposed media release developed by the Vendor.

After Medicaid approval, _____ shall provide the necessary notices to the recipient, prominent media outlet, or the Secretary of Health and Human Services (HHS) to report _____ data breaches as required by 45 C.F.R. Part 164, Subpart D. If recipient addresses are needed for the recipient notices, _____ shall work with designated Medicaid staff to secure current mailing addresses for the recipients. _____ shall reimburse Medicaid for all cost associated with providing recipient addresses.

_____ shall pay all fines or penalties imposed by HHS under 45 C.F.R. Part 160 HIPAA Administrative Simplification: Enforcement rule for breaches made by any employee, officer, or agent of _____.

_____ shall pay all costs associated with notifying recipients, media outlets, and HHS.

_____ shall comply with all federal HIPAA Privacy and Security Rules for a covered entity if _____ is a covered entity. If _____ is not a covered entity, it shall comply with the HIPAA Privacy and Security Rules as if it was a covered entity.

_____ shall designate a Privacy and Security Officer as required by HIPAA regulations. One individual may serve in the capacity of both Privacy and Security Officer. _____ shall obtain Medicaid approval of their Privacy and Security Officer designee(s).

_____ shall perform a technical and nontechnical security evaluation based on the standards outlined in 45 C.F.R. Part 164, Subpart C Security Standards for the Protection of Electronic Protected Health Information to identify deficiencies that led to the data breach.

_____ shall correct all deficiencies identified by the security evaluation to bring _____ into compliance with the HIPAA Security Rule and report the corrected deficiencies to Medicaid prior to another data exchange under this agreement.

XV. Compliance.

It is the responsibility of _____ to take all reasonable steps to ensure compliance with the conditions set out in this agreement, and to ensure that unacceptable use of Medicaid data does not occur.

All parties shall comply with the provisions of the Health Insurance Portability and Accountability Act of 1996 and any implementing regulations as adopted.

Additionally, it is incumbent upon _____ to inform its officers and employees of penalties for improper disclosure implied by the Privacy Act of 1974, 5 U. S. C. 552a. Specifically, 5 USC 552a (i) (1), which is made applicable to contractors by 5 U. S. C. 552a (m) (1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses that material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

Each officer or employee of _____ or its subcontractors or agents to whom Social Security information is or may be disclosed shall be notified in writing by your

Agency that such information can only be used for authorized purposes and to that extent and any other unauthorized use herein constitutes a felony punishable upon conviction by a fine of as much as $5,000.00 or imprisonment for as long as five years, or both, together with the cost of prosecution. Your agency shall also notify each individual that further disclosure of Social Security information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000.00 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC Section 7213 and 7431 and set forth at 26 C.F.R. 301.6103(n).

XVI. Information Systems/Technology Manager Authority.

Medicaid Authority:
Marty Redden
Chief Information Technology Officer
501 Dexter Ave.| Montgomery, AL 36103
334-353-3714
Email: Marty.Redden@medicaid.alabama.gov

_____ Authority:
Name:
Title:
Address:
Phone:
Email:

XVII. Signatures.

In witness whereof, the parties hereto have executed this agreement as evidenced by their signatures below.

_____	_____
Stephanie McGee Azar, Commissioner, Alabama Medicaid Agency	Date
_____	_____
Name & title of signing entity authority Entity name	Date
_____	_____
Legal Counsel Alabama Medicaid Agency	Date
_____	_____
Entity Legal/General Counsel Entity name	Date