

**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 _____ has 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, pursuant to Sections 22-6-220, *et seq.* of the Alabama Code, is transforming Medicaid by providing for the delivery of medical services to Medicaid beneficiaries on a managed care basis through the Alabama Coordinated Health Network (ACHN), a case management entity. _____ has been given notice of intent to award and as such must meet specific requirements to maintain that status and move forward as a fully certified ACHN. To meet these benchmarks, _____ is in need of Medicaid claims data to complete the process of becoming a fully certified ACHN.

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 terminated by agreement of both parties or upon thirty (30) days written notice to the other party. The effective date of termination will be on the first day of the month following expiration of the thirty (30) day notice period. This agreement may be amended as required, provided that such is in writing and signed by both parties.

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.*

_____ 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 without the prior approval of the Commissioner of Medicaid, and then only to individuals expressly authorized to review such information under federal or state laws.. 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. Consistent with section 3.5 of the associated Business Associate Agreement, _____ will ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information

Consistent with Section 6 of the underlying Memorandum of Understanding, all proposed publications of any kind or public presentations or disseminations, including internally, that are derived from the data generated by this exchange of information must receive prior written approval from the Commissioner of Medicaid. The Alabama Medicaid Agency retains final editorial rights to all final products that are derived from the data exchanged pursuant to this agreement. _____ understands that any damages arising out of unauthorized access or

disclosure, or misuse of this data on _____'s behalf will be the responsibility of _____.

If _____, its 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 of law that may be available.

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

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) days 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 transmission meets 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.

Medicaid has given a notice of intent to award to _____ pursuant to Medicaid’s efforts to provide for the delivery of medical services to Medicaid beneficiaries on a managed care basis through the Alabama Coordinated Health Network (ACHN) case management entity. _____ must meet specific requirements to move forward as a fully certified ACHN. To meet these benchmarks, _____ is in need of Medicaid data for use in becoming a fully certified ACHN.

XI. Description of Data.

Medicaid and _____ shall use test data files and limited data sets of expected population of the ACHN to assist _____ in completing its Readiness Assessment.

Technical Contacts for Data Format and Content

Contact Name & Title	Contact Information	Contact for Questions Regarding:
		Data content, format, and submission
		Data content, format, and submission

Medicaid Technical Contacts for Data Format and Content

Contact Name & Title	Contact Information	Contact for Questions Regarding:
Drew Nelson, Epidemiologist, Director of Quality Assurance	334-332-7663 Drew.Nelson@Medicaid.Alabama.gov	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 shall be transmitted via either the Agency’s or _____’s SFTP site.

Email Notification List (optional)

Email Contact Name & Title	Contact Information

Medicaid Email Notification List (optional)

Email Contact Name & Title	Contact Information
Drew Nelson, Epidemiologist, Director of Quality Assurance	334-332-7663 Drew.Nelson@Medicaid.Alabama.gov
Michael E. Kelley, Director Application Development and Support	334-353-4106 Michael.Kelley@Medicaid.Alabama.gov

XIII. Data Sharing Financial Obligations.

_____ and Medicaid agree that this agreement provides for mutual consideration to the parties. There is no payment required by either of the parties pursuant to this Agreement.

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 unsecured 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 _____'s toll-free number or direct number, email address, Web site, or postal address.
- A proposed media release developed by _____.

After Medicaid approval, _____ shall provide the necessary notices to the recipient, prominent media outlet, and/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 were 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 U.S.C. § 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 I.R.C. Section 7213 and 7431 and set forth at 26 C.F.R. § 301.6103(n).

XVI. Information Systems/Technology Manager Authority.

Medicaid Authority:

Mason Tanaka
Chief Information Officer
501 Dexter Ave. | Montgomery, AL 36103
334-353-3714
Email: Mason.Tanaka@medicaid.alabama.gov

_____ Authority:

No.

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

**MEMORANDUM OF UNDERSTANDING
BETWEEN**

AND

THE ALABAMA MEDICAID AGENCY

THIS AGREEMENT is entered into, by and between, the Alabama Medicaid Agency (hereinafter referred to as Medicaid) and _____ (hereinafter referred to as Contractor), regarding the exchange of data to conduct an analysis of state wide Medicaid claims data in order to complete Readiness Assessment criteria as necessary to achieve the requirements of the Alabama Coordinated Health Network (ACHN); and

WHEREAS, Contractor and Medicaid agree to the exchange of data for the purpose of analyzing state Medicaid claims data to pursue options for collaboration with respect to the establishment of an Alabama Coordinated Health Network and agree to the following terms and conditions:

1. Medicaid shall transfer data, as described in the attached Data Sharing Agreement, Attachment A, to the Contractor in return for the Contractor delivering to Medicaid periodic written reports regarding the data and its utilization in accomplishing the required ACHN Readiness Assessment. Contractor agrees to provide the first report to Medicaid within six months of signing this agreement. Additional periodic reports will be provided to Medicaid by Contractor at a mutually agreeable time. All reports should be electronically delivered to Drew Nelson, Director of Quality Assurance and/or his designee or successor unless a different contact is named by the Commissioner of Alabama Medicaid ("Medicaid Contact").
2. The Contractor and Medicaid agree to enter into a Business Associate Agreement and acknowledge that data exchanged may only be used for the purposes expressly provided for within the Business Associate Agreement and this Memorandum of Understanding.
3. This Memorandum of Understanding shall be effective immediately upon execution and, except as otherwise provided above, shall remain in effect until terminated by agreement of both parties or upon thirty (30) days written notice to the other party. The effective date of termination will be on the first day of the month following expiration of the thirty (30) day notice period. This agreement may be amended as required, provided that such is in writing and signed by both parties.
4. Contractor and Medicaid agree that this Memorandum of Understanding provides for mutual consideration to the parties. There is no payment required by either of the parties pursuant to this Agreement.
5. Contractor acknowledges and understands that this contract is not effective until it has received all requisite state government approvals and Contractor shall not receive any of the data to be exchanged pursuant to this MOU until all requisite approvals have been obtained.

Contract No: _____

6. Contractor shall submit all completed analyses, statistics, reports, and/or conclusions, including accompanying methodologies to the Medicaid Contact as stated in Section One (1) of this MOU. No publications of any kind or public presentations or disseminations, including internally, may be derived from the data generated by this exchange of information without prior written approval from the Commissioner of Medicaid. The Alabama Medicaid Agency retains final editorial rights to all final products that are derived from the data exchanged pursuant to this agreement.

7. Contractor agrees to comply with the Data Sharing agreement attached hereto as Attachment A.

8. Contractor agrees to comply with the Business Associate Agreement attached here to as Attachment B.

9. Pursuant to Ala. Code §31-13-9(k), by signing this contract, the contracting parties affirm, for the duration of the agreement, that they will not violate federal immigration law or knowingly employ, hire for employment, or continue to employ an unauthorized alien within the state of Alabama. Furthermore, a contracting party found to be in violation of this provision shall be deemed in breach of the agreement and shall be responsible for all damages resulting therefrom.

Alabama Medicaid Agency

This agreement has been reviewed for and is approved as to content.

Stephanie McGee Azar
Commissioner

SIGNATURE AUTHORITY
TITLE

Date Signed

Date Signed

This agreement has been reviewed for legal form and complies with all applicable laws, rules, and regulations of the State of Alabama governing these matters.

Legal Counsel

Legal Counsel

**ALABAMA MEDICAID AGENCY
BUSINESS ASSOCIATE AGREEMENT**

This Agreement is made effective the _____ day of _____, 20____, by and between the Alabama Medicaid Agency (“Covered Entity”), an agency of the State of Alabama, and _____ (“Business Associate”) (collectively the “Parties”).

1. BACKGROUND

- 1.1. Business Associate agrees to perform the following services for or on behalf of Covered Entity. The State of Alabama, pursuant to Sections 22-6-220, *et seq.* of the Alabama Code, is transforming Medicaid by providing for the delivery of medical services to Medicaid beneficiaries on a managed care basis through the Alabama Coordinated Health Network (ACHN). _____ has been given notice of intent to award and as such must meet specific requirements to maintain that status and move forward as a fully certified ACHN. To meet these benchmarks, contractor is in need of Medicaid claims data to complete the process of becoming a fully certified ACHN.
- 1.2. The relationship between Covered Entity and Business Associate is such that the Parties believe Business Associate is or may be a “business associate” within the meaning of the HIPAA Rules (as defined below).
- 1.3. The Parties enter into this Business Associate Agreement with the intention of complying with the HIPAA Rules allowing a covered entity to disclose protected health information to a business associate, and allowing a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.

2. DEFINITIONS

2.1 General Definitions

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Electronic Protected Health Information, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

2.2 Specific Definitions

- 2.2.1 Business Associate. “Business Associate” shall generally have the same meaning as the term “business associate” at 45 C.F.R. § 160.103

2.2.2 Covered Entity. “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 C.F.R. § 160.103.

2.2.3 HIPAA Rules. “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164.

3. OBLIGATIONS OF BUSINESS ASSOCIATE

Business Associate agrees to the following:

- 3.1** Use or disclose PHI only as permitted or required by this Agreement or as Required by Law.
- 3.2** Use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this Agreement. Further, Business Associate will implement administrative, physical and technical safeguards (including written policies and procedures) that reasonably and appropriately protect the confidentiality, integrity and availability of electronic PHI that it creates, receives, maintains or transmits on behalf of Covered Entity as required by Subpart C of 45 C.F.R. Part 164.
- 3.3** Mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.
- 3.4** Report to Covered Entity within five (5) business days any use or disclosure of PHI not provided for by this Agreement of which it becomes aware.
- 3.5** Ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information in accordance with 45 C.F.R. § 164.502(e)(1)(ii) and § 164.308(b)(2), if applicable.
- 3.6** Provide Covered Entity with access to PHI within thirty (30) business days of a written request from Covered Entity, in order to allow Covered Entity to meet its requirements under 45 C.F.R. § 164.524, access to PHI maintained by Business Associate in a Designated Record Set.
- 3.7** Make amendment(s) to PHI maintained by Business Associate in a Designated Record Set that Covered Entity directs or agrees to, pursuant to 45 C.F.R. § 164.526 at the written request of Covered Entity, within thirty (30) calendar days after receiving the request.
- 3.8** Make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received by the Business Associate on behalf of, Covered Entity, available to Covered Entity or to the Secretary within five (5) business days after receipt of written notice or as designated by the Secretary for purposes of determining compliance with the HIPAA Rules.

- 3.9** Maintain and make available the information required for Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI as necessary to satisfy the Covered Entity's obligations under 45 C.F.R. § 164.528.
- 3.10** Provide to the Covered Entity, within thirty (30) days of receipt of a written request from Covered Entity, the information required for Covered Entity to respond to a request by an Individual or an authorized representative for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.
- 3.11** Maintain a comprehensive security program appropriate to the size and complexity of the Business Associate's operations and the nature and scope of its activities as defined in the Security Rule.
- 3.12** Notify the Covered Entity within five (5) business days following the discovery of a breach of unsecured PHI on the part of the Contractor or any of its sub-contractors, and
- 3.12.1 Provide the Covered Entity the following information:
- 3.12.1(a) The number of recipient records involved in the breach.
 - 3.12.1(b) A description of what happened, including the date of the breach and the date of the discovery of the breach if known.
 - 3.12.1(c) 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).
 - 3.12.1(d) Any steps the individuals should take to protect themselves from potential harm resulting from the breach.
 - 3.12.1(e) A description of what the Business Associate is doing to investigate the breach, to mitigate harm to individuals and to protect against any further breaches.
 - 3.12.1(f) Contact procedures for individuals to ask questions or learn additional information, which shall include the Business Associate's toll-free number, email address, Web site, or postal address.
 - 3.12.1(g) A proposed media release developed by the Business Associate.
- 3.12.2 Work with Covered Entity to ensure the necessary notices are provided to the recipient, prominent media outlet, or to report the breach to the Secretary of Health and Human Services (HHS) as required by 45 C.F.R. Part 164, Subpart D.;
- 3.12.3 Pay the costs of the notification for breaches that occur as a result of any act or failure to act on the part of any employee, officer, or agent of the Business Associate;
- 3.12.4 Pay all fines or penalties imposed by HHS under 45 C.F.R. Part 160, "HIPAA Administrative Simplification: Enforcement Rule" for breaches that occur as a result of any act or failure to act on the part of any employee, officer, or agent of the Business Associate.

3.12.5 Co-ordinate with the Covered Entity in determining additional specific actions that will be required of the Business Associate for mitigation of the breach.

4. PERMITTED USES AND DISCLOSURES

Except as otherwise limited in this Agreement, Business Associate may

- 4.1.** Use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as agreed to, provided that such use or disclosure would not violate the Subpart E of 45 C.F.R. Part 164 if done by Covered Entity;
- 4.2.** Use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
- 4.3.** Disclose PHI for the proper management and administration of the Business Associate, provided that:
 - 4.3.1** Disclosures are Required By Law; or
 - 4.3.2** Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
- 4.4** Use PHI to provide data aggregation services to Covered Entity as permitted by 42 C.F.R. § 164.504(e)(2)(i)(B).

5. REPORTING IMPROPER USE OR DISCLOSURE

The Business Associate shall report to the Covered Entity within five (5) business days from the date the Business Associate becomes aware of:

- 5.1** Any use or disclosure of PHI not provided for by this agreement
- 5.2** Any Security Incident and/or breach of unsecured PHI

6. OBLIGATIONS OF COVERED ENTITY

The Covered Entity agrees to the following:

- 6.1** Notify the Business Associate of any limitation(s) in its notice of privacy practices in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect Alabama Medicaid's use or disclosure of PHI.
- 6.2** Notify the Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect the Business Associate's use or disclosure of PHI.
- 6.3** Notify the Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect the Business Associate's use or disclosure of PHI.
- 6.4** Not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

6.5 Provide Business Associate with only that PHI which is minimally necessary for Business Associate to provide the services to which this agreement pertains.

7. TERM AND TERMINATION

7.1 Term. The Term of this Agreement shall be effective as of the effective date stated above and shall terminate when the Business Associate no longer provides agreed upon services to the Covered Entity.

7.2 Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity may, at its option:

7.2.1 Provide an opportunity for Business Associate to cure the breach or end the violation, and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

7.2.2 Immediately terminate this Agreement; or

7.2.3 If neither termination nor cure is feasible, report the violation to the Secretary as provided in the Privacy Rule.

7.3 Effect of Termination.

7.3.1 Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.

7.3.2 In the event that Business Associate determines that the PHI is needed for its own management and administration or to carry out legal responsibilities, and returning or destroying the PHI is not feasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction not feasible. Business Associate shall:

7.3.2(a) Retain only that PHI which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;

7.3.2(b) Return to covered entity or, if agreed to by covered entity, destroy the remaining PHI that the business associate still maintains in any form;

7.3.2(c) Continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the PHI;

7.3.2(d) Not use or disclose the PHI retained by business associate other than for the purposes for which such PHI was retained and subject to the same conditions set out at Section 4, "Permitted Uses and Disclosures" which applied prior to termination; and

7.3.2(e) Return to covered entity or, if agreed to by covered entity, destroy the PHI retained by business associate when it is no longer needed by business

associate for its proper management and administration or to carry out its legal responsibilities.

7.4 Survival

The obligations of Business Associate under this Section shall survive the termination of this Agreement.

8. GENERAL TERMS AND CONDITIONS

- 8.1** Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the HIPAA Rules.
- 8.2** A breach of this Agreement by Business Associate shall be considered sufficient basis for Covered Entity to terminate the services of the Business Associate.
- 8.3** The Parties agree to take such action as is necessary to amend this Agreement from time to time for Covered Entity to comply with the requirements of the HIPAA Rules.

IN WITNESS WHEREOF, Covered Entity and Business Associate have executed this Agreement effective on the date as stated above.

ALABAMA MEDICAID AGENCY

Signature: _____

Printed Name: Clay Gaddis

Title: Privacy Officer

Date: _____

BUSINESS ASSOCIATE

Signature: _____

Printed Name: _____

Title: _____

Date: _____