

BUSINESS ASSOCIATE AGREEMENT
BETWEEN
THE ALABAMA DEPARTMENT OF PUBLIC HEALTH
AND

This Agreement is entered into by and between the **Alabama Department of Public Health**, (“**Covered Entity**”), an agency of the State of Alabama, and

(“**Business Associate**”) and is effective as of _____.

WHEREAS, Covered Entity and Business Associate have entered into a Contract (“Contract”) in which Business Associate has agreed to provide certain services to Covered Entity. In connection with that Contract, Business Associate creates, receives, maintains or transmits Protected Health Information (“PHI”) from, to, or on behalf of Covered Entity. This information is protected by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009, (the “HITECH Act”), and the associated regulations promulgated by the Secretary (“HIPAA Rules”).

WHEREAS, it is desirable, in order to further the continued efficient operations of Covered Entity to disclose to Business Associate certain PHI, and Business Associate has certain responsibilities with respect to that PHI; and

WHEREAS, in light of the foregoing requirements of HIPAA, the HITECH Act, and the HIPAA Rules, Business Associate and Covered Entity agree to be bound by the terms and conditions of this Agreement.

NOW THEREFORE, in consideration of the mutual promises herein, the parties agree as follows:

1. Definitions.

a. Catch-all definition: The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Designated Record Set, Disclosure, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

b. **Business Associate** shall have the meaning given to such term in 45 CFR § 160.103.

c. **Covered Entity** shall have the meaning given to such term in 45 CFR § 160.103

d. **HIPAA Rules** means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Parts 160 and 164.

2. **Permitted Uses and Disclosures.**

a. **Purposes.** Except as otherwise limited in this Agreement, Business Associate may only use or disclose PHI to perform functions, activities or services for, or on behalf of, Covered Entity as specified in the Contract, provided that such use or disclosure would not violate HIPAA or applicable state law if done by Covered Entity, or the minimum necessary and related Privacy and Security policies and procedures of Covered Entity. All such uses and disclosures shall be consistent with the minimum necessary requirements of HIPAA. Business Associate is directly liable under HIPAA for the impermissible Use or Disclosure of PHI it handles on behalf of Covered Entity.

b. **De-Identified Data.** Business Associate is not authorized to de-identify PHI or to use or disclose any de-identified PHI of Covered entity except as otherwise provided in the Contract. If de-identification is specified in the Contract, Business Associate shall de-identify the information in accordance with 45 CFR 164.514(a) – (c).

c. **Use for Administration of Business Associate.** Except as otherwise limited in this Agreement, the Business Associate may use PHI for the proper management and administration of Business Associate, or to carry out the legal responsibilities of Business Associate.

d. **Disclosure for Administration of Business Associate.** Except as otherwise limited in this Agreement, Business Associate may disclose PHI for the proper management and administration of Business Associate, provided that (i) the disclosure is Required by Law; or (ii) the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the PHI will remain confidential and be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person; and, (iii) the person agrees to notify the Business Associate and Covered Entity of any instances of which it is aware in which the confidentiality of the information has been breached.

3. **Covered Entity to Inform Business Associate of Privacy Practices and Restrictions.**

a. **Notice of Privacy Practices.** Covered Entity shall notify Business Associate

of any limitation(s) in the Notice of Privacy Practices of Covered Entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of protected health information.

b. **Restriction on Use or Disclosure.** Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that covered entity has agreed to or is required to abide by under 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

c. **Revocation of Permission to Use or Disclose.** Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

4. **Permissible Requests by Covered Entity.** Except as set forth in Section 2 of this Agreement, Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Covered Entity.

5. **Obligations of Business Associate.**

a. **Use and Disclosure.** Business Associate agrees not to use or disclose PHI other than as permitted or required by the Contract or as Required by Law. Business Associate shall comply with the provisions of the Agreement relating to privacy and security of PHI and all present and future provisions of HIPAA that relate to the privacy and security of PHI that are applicable to Covered Entity and/or Business Associate.

b. **Appropriate Safeguards.** Business Associate will use appropriate safeguards as are necessary to prevent the use or disclosure of PHI, except as provided for in this Agreement, and comply with Subpart C of 45 CFR Part 164 with respect to Electronic Protected Health Information. Business Associate represents and warrants that Business Associate:

i. Has implemented and will continue to maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of PHI as required by the Security Rule; and

ii. Will comply with 74 FR 19006 Guidance Specifying the Technologies and Methodologies That Render PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII. With regard to electronic PHI not covered by the Guidance published at 74 FR 19006, Business Associate will protect electronic PHI at rest and in transit through encryption that complies with State of Alabama Information Technology Policy 683-00: Encryption.

- iii. Shall ensure that any agent or subcontractor that creates, receives, maintains, or transmits PHI on behalf of the Business Associate agrees to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information.

c. **Breach Notification.** Business Associate shall promptly, and in any event within three (3) business days, report to Covered Entity any of the following:

- i. Any use or disclosure of PHI not permitted by this Business Associate Agreement of which Business Associate becomes aware;
- ii. Any Security Incident of which Business Associate becomes aware; and
- iii. The discovery of a Breach of Unprotected Health Information.

A Breach is discovered as of the first day on which the Breach is known, or reasonably should have been known, to Business Associate or any employee, officer or agent of Business Associate. Any notice of a Security Incident or Breach of Unsecured Protected Health Information shall include (1) the date of discovery; (2) the data elements involved; (3) the identification of each Individual whose PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired or disclosed during such Security Incident or Breach; (4) where the PHI or confidential data is believed to have been improperly transmitted; (5) the probable cause(s) of the improper use or disclosure; (6) a description of the proposed plan for preventing similar future incidents; and (7) whether any federal or state laws requiring breach notification are triggered. Any such notice shall be directed to Covered Entity's Privacy Officer.

d. **Investigation.** Business Associate shall reasonably cooperate and coordinate with Covered Entity in the investigation of any violation of the requirements of this Business Associate Agreement and/or any Security Incident or Breach.

e. **Mitigation.** Business Associate agrees to mitigate, to the extent practical, any harmful effect that is known to Business Associate or its employees, officers, Subcontractors or agents of a use or disclosure of PHI by Business Associate in violation of this Agreement. Business Associate shall keep Covered Entity fully apprised of all mitigation efforts, and all associated costs shall be borne by the Business Associate. This includes, but is not limited to, costs associated with notifying affected individuals.

f. **Reports and Notices.** Business Associate shall reasonably cooperate and coordinate with Covered Entity in the preparation of any reports or notices to the Individual or other authorities required to be made under HIPAA, the HITECH Act, HIPAA Rules, or any other federal or state laws. Any such reports or notices shall be subject to the prior written approval of Covered Entity.

g. **Agents/Subcontractors.** Business Associate agrees to ensure that any agent and/or subcontractor that creates, receives, maintains or transmits PHI on behalf

of Business Associate agrees in writing to restrictions and conditions at least as stringent as those that apply to Business Associate pursuant to this Agreement with respect to such PHI. Failure to include such requirement in any subcontract or agreement may result in Covered Entity's termination of the Agreement. If Business Associate becomes aware of a pattern of activity or practice of an agent and/or subcontractor that constitutes a material breach or violation of any such restrictions or conditions, Business Associate shall take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement with such agent and/or subcontractor.

h. **Access to Designated Record Sets.** To the extent that Business Associate possesses or maintains PHI in a Designated Record Set, Business Associate agrees to provide access, at the request of Covered Entity, in the time, format and manner reasonably requested by Covered Entity to PHI in a Designated Record Set to enable Covered Entity to fulfill its obligations under HIPAA. If an Individual makes a request directly to Business Associate, Business Associate shall notify Covered Entity of the request within three (3) business days of such request and will cooperate with Covered Entity and allow Covered Entity to send the response to the Individual.

i. **Amendment to Designated Record Sets.** To the extent that Business Associate possesses or maintains PHI in a Designated Record Set, Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to at the request of Covered Entity or an Individual, and in the time and manner reasonably requested by Covered Entity. If an Individual makes a request to amend PHI directly to Business Associate, Business Associate shall notify Covered Entity of the request within three (3) business days of such request and will cooperate with Covered Entity and allow Covered Entity to send the response to the Individual.

j. **Access to Books and Records.** Business Associate agrees to make its internal practices, books, and records, including policies and procedures relating to the use and disclosure of PHI, as well as the PHI, received from, or created or received by Business Associate on behalf of Covered Entity available to Covered Entity, or to the Secretary, for the purpose of the Secretary determining Covered Entity's or Business Associate's compliance with HIPAA. Business Associate also agrees to make these records available to Covered Entity, or Covered Entity's contractor, for periodic audit of Business Associate's compliance with the Privacy and Security Rules. Upon Covered Entity's request, the Business Associate shall provide proof of compliance with HIPAA and HITECH data privacy/protection guidelines, certification of a secure network and other assurance relative to compliance with the Privacy and Security Rules. This section shall also apply to Business Associate's subcontractors, if any.

k. **Accountings.** Business Associate agrees to document disclosures of PHI and information related to such disclosures that would be required for Covered Entity

to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with HIPAA. This should include a process that allows for an accounting to be collected and maintained by Business Associate and its agents or subcontractors for at least six (6) years from the date of disclosure, or longer if required by state law. At a minimum, such documentation shall include:

- i. the date of disclosure;
- ii. the name of the entity or person who received the PHI, and if known, the address of the entity or person;
- iii. a brief description of the PHI disclosed; and
- iv. a brief statement of purposes of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure.

l. Requests for Accountings. Business Associate agrees to provide to Covered Entity or an Individual, in the time and manner reasonably requested by Covered Entity, information collected in accordance with Section 5.k. of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with HIPAA. If an Individual makes a request for an accounting of disclosures of PHI directly to Business Associate, Business Associate shall notify Covered Entity of the request within three (3) business days of such request and will cooperate with Covered Entity and allow Covered Entity to send the response to the Individual. The duty of the Business Associate and its agents and subcontractors to assist Covered Entity with any HIPAA required accounting of disclosures survives the termination of the Contract.

m. Privacy Requirements. To the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, Business Associate shall comply with the requirements of Subpart E that apply to the covered Entity in the performance of such obligation(s).

n. Data Ownership. The PHI, and any related information created or received from or on behalf of Covered Entity, is and shall remain the property of Covered Entity. Neither Business Associate nor its agents or subcontractors shall hold any data ownership rights with respect to the PHI.

o. Assistance in Litigation or Administrative Proceedings. Business Associate shall make itself and any subcontractors, workforce or agents assisting Business Associate in the performance of its obligations under this Agreement, available to Covered Entity at no cost to Covered Entity, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against Covered Entity, its officers or employees based upon claimed violations of HIPAA, the HIPAA Regulations or other laws relating to security and privacy, which involves action or inaction by Business Associate, except where Business Associate or its subcontractor, workforce or agent is a named as an

adverse party.

p. **Remuneration for PHI.** Business Associate is prohibited from directly or indirectly receiving any remuneration in exchange for an individual's PHI without the written authorization of the individual. Business Associate will refrain from marketing activities that would violate HIPAA, including specifically Section 13406 of the HITECH Act.

6. **Term and Termination.**

a. **Term.** This Agreement shall be effective as of the date of the Contract and shall terminate upon termination of the Contract or on the date Covered Entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

b. **Termination for Cause.** Business Associate authorizes termination of this Agreement by Covered Entity, if Covered Entity determines Business Associate has violated a material term of the Agreement. Covered Entity may, at its sole discretion, allow Business Associate a reasonable period of time to cure the material breach before termination.

c. **Duties at Termination.**

i. Upon termination of the Contract for any reason, Business Associate shall return or destroy, at Covered Entity's option, all PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that the Business Associate still maintains in any form. Business Associate shall retain no copies of the PHI. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate.

ii. In the event that Business Associate determines that returning or destroying the PHI is not feasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction of the PHI infeasible, for so long as Business Associate maintains such PHI. This shall also apply to all agents and subcontractors of Business Associate.

d. **Judicial or Administrative Proceedings.** Covered Entity may terminate this Agreement, effective immediately, if (1) Business Associate is named as a defendant in a criminal proceeding for a violation of HIPAA, the HIPAA Regulations, or other security or privacy laws or (2) a finding or stipulation that Business Associate has violated any standard or requirement of HIPAA, the HIPAA Regulations, or other security or privacy laws is made in any administrative or civil

proceeding in which Business Associate is a party or has been joined. Business Associate shall be subject to prosecution by the Department of Justice for violations of HIPAA/HITECH and shall be responsible for any and all costs associated with prosecution.

e. **Notices.** Any notices required under this Agreement will be sent in writing via certified mail, return receipt requested and also via electronic mail.

For Business Associate:

For Covered Entity:

Pamela Kendrick, CHPC
Privacy Officer
Alabama Department of Public
Health
201 Monroe Street
Montgomery, AL 36104
Phone: (334) 206-9324
Fax: (334) 206-5874
pamela.kendrick@adph.state.al.us

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

7. Miscellaneous.

a. **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 Covered Entity, Business Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

b. **Regulatory References.** A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

c. **Interpretation.** Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

d. **Amendment.** The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA rules and any other applicable law.

IN WITNESS WHEREOF, the authorized representatives of the parties sign effective the date above.

BUSINESS ASSOCIATE

COVERED ENTITY

Alabama Department of Public Health

By: _____

By: _____

Printed Name: _____

Printed Name: _____

Title: _____

Title: _____