BUSINESS ASSOCIATE AGREEMENT

BETWEEN

THE MOBILE COUNTY HEALTH DEPARTMENT

AND

_____

This Agreement is entered into by and between the **Mobile County Health Department,** hereinafter **"Department,"** and _____, hereinafter **"Business Associate,"** and is effective as of _____, 2015 ("Effective Date").

The Business Associate performs certain services on behalf of or for the Department pursuant to the underlying Agreement, whether oral or written, that requires the exchange of information including protected health information protected by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the American Recovery and Reinvestment Act of 2009 (Pub. L. No. 111-5) (the "HITECH Act"), any associated regulations and the federal regulations published at 45 CFR parts 160 and 164 (sometimes collectively referred to as "HIPAA"). The Department is a *"Covered* Entity" as that term is defined in HIPAA, and the parties to the underlying Agreement are entering into this Agreement to establish the responsibilities of both parties regarding HIPAA-covered information and to bring the underlying Agreement into compliance with HIPAA.

Whereas it is desirable, in order to further the continued efficient operations of the Department to disclose to its Business Associate certain information which may contain confidential individually identifiable health information (hereafter, Protected Health Information or PHI); and

Whereas, it is the desire of both parties that the confidentiality of the PHI disclosed hereunder be maintained and treated in accordance with all applicable laws relating to confidentiality, including the Privacy and Security Rules, the HITECH Act and its associated regulations, and the parties do agree to at all times treat the PHI and interpret this Agreement consistent with that desire.

NOW THEREFORE: the parties agree that in consideration of the mutual promises herein, in the Agreement, and of the exchange of PHI hereunder that:

1. **Definitions**. Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

a. **Department Privacy Officer** shall mean the Department's HIPAA Privacy Officer.

b. **Agent** shall mean those person(s) who are agent(s) of the Business Associate, in accordance with the Federal common law of Department, as referenced in 45 CFR § 160.402(c).

c. **Breach** shall mean the acquisition, access, use of disclosure of protected health information which compromises the security of privacy of such information, except as excluded in the definition of Breach in 45 CFR § 164.402.

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

e. **HITECH Act** shall mean the Health Information Technology for Economic and Clinical Health Act. Public Law No. 111-05. 111th Congress (2009).

f. **Privacy Rule** means the Standards for Privacy of Individually Identifiable Health Information found at 45 CFR Parts 160 and 164.

g. **Protected Health Information or PHI** shall have the meaning given to such term in 45 CFR § 160.103 limited to the information created or received by Business Associate from or on behalf of Department.

h. **Security Incident** means any known successful or unsuccessful attempt by an authorized or unauthorized individual to inappropriately use, disclose, modify, access, or destroy any information or interference with system operations in an information system.

i. **Security Rule** means the Security Standards for the Protection of Electronic Protected Health Information found at 45 CFR Parts 160 and 164.

j. **Subcontractor** means a person to whom a Business Associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such Business Associate.

2. Permitted Uses and Disclosures.

a. PHI Described. This means PHI created, received, maintained or transmitted on behalf of the Department by the Business Associate. This PHI is governed by this Agreement and is limited to the minimum necessary, to complete the tasks or to provide the services associated with the terms of the underlying Agreement, and is generally described in Appendix A.

b. Purposes. Except as otherwise limited in this Agreement, Business Associate may use or disclose the PHI on behalf of, or to provide services to, Department for the purposes necessary to complete the tasks, or provide the services, associated with, and required by the terms of the underlying Agreement, or as required by law, if such use or

disclosure of the PHI would not violate the Privacy or Security Rules or applicable state law if done by Department or Business Associate, or violate the minimum necessary and related Privacy and Security policies and procedures of the Department. The Business Associate is directly liable under HIPAA for impermissible uses and disclosures of the PHI it handles on behalf of Department.

c. **Further Uses and Disclosures.** Except as otherwise limited in this Agreement, the Business Associate may disclose PHI to third parties for the purpose of its own proper management and administration, or as required by law, provided that (i) the disclosure is required by law; or (ii) the Business Associate has obtained from the third party reasonable assurances that the PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the third party by the Business Associate; and, (iii) an agreement to notify the Business Associate and Department of any instances of which it (the third party) is aware in which the confidentiality of the information has been breached. To the extent practical, the information should be in a limited data set or the minimum necessary information pursuant to 45 CFR § 164.502, or Business Associate will take other measures as necessary to satisfy the Department's obligations under 45 CFR § 164.502.

3. Obligations of Business Associate.

a. Stated Purposes Only. The PHI may not be used by the Business Associate for any purpose other than as stated in this Agreement or as required or permitted by law.

b. Limited Disclosure. The PHI is confidential and will not be disclosed by the Business Associate other than as stated in this Agreement or as required or permitted by law. Business Associate is prohibited from directly or indirectly receiving any remuneration in exchange for an individual's PHI unless Department gives written approval and the individual provides a valid authorization. Business Associate will refrain from marketing activities that would violate HIPAA, including specifically Section 13406 of the HITECH Act. Business Associate will report to Department any use or disclosure of the PHI, including any Security Incident not provided for by this Agreement of which it becomes aware.

c. Safeguards. The Business Associate will use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of the PHI, except as provided for in this Agreement. This shall include, but not be limited to:

i. Limitation of the groups of its workforce and agents, to whom the PHI is disclosed to those reasonably required to accomplish the purposes stated in this Agreement, and the use and disclosure of the minimum PHI necessary or a Limited Data Set;

ii. Appropriate notification and training of its workforce and agents in order to

protect the PHI from unauthorized use and disclosure;

iii. Maintenance of a comprehensive, reasonable and appropriate written PHI privacy and security program that includes administrative, technical and physical safeguards appropriate to the size, nature, scope and complexity of the Business Associate's operations, in compliance with the Security Rule;

iv. In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, 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.

d. Compliance With Law. The Business Associate will not use or disclose the PHI in a manner in violation of existing law and specifically not in violation of laws relating to confidentiality of PHI , including but not limited to, the Privacy and Security Rules.

e. Mitigation. Business Associate agrees to mitigate, to the extent practicable, any harmful *effect* that is known to Business Associate of a use or disclosure of the PHI by Business Associate in violation of the requirements of this Agreement, and report its mitigation activity back to the Department.

f. Support of Individual Rights.

i. Access to PHI. Business Associate shall make the PHI maintained by Business Associate or its agents or subcontractors in Designated Record Sets available to Department for inspection and copying, and in electronic format, if requested, within five (5) days of a request by Department to enable Department to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR § 164.524 and consistent with Section 13405 of the HITECH Act

ii. Amendment of PHI. Within five (5) days of receipt of a request from Department for an amendment of the PHI or a record about an individual contained in a Designated Record Set, Business Associate or its agents or subcontractors shall make such PHI available to Department for amendment and incorporate any such amendment to enable Department to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR § 164.526.

iii. Accounting Rights. Within five (5) days of notice of a request for an accounting of disclosures of the PHI, Business Associate and its agents or subcontractors shall make available to Department the documentation required to provide an accounting of disclosures to enable Department to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR §164.528 and consistent with Section 13405 of the HITECH Act Business Associate agrees to document disclosures of the PHI and information related to such disclosures as would be required for Department to respond to a request by an individual for an

accounting of disclosures of PHI in accordance with 45 CFR § 164.528. 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:

- the date of disclosure;
- the name of the entity or person who received the PHI, and if known, the address of the entity or person;
- a brief description of the PHI disclosed; and
- 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.

iv. Request for Restriction. Under the direction of the Department, abide by any individual's request to restrict the disclosure of PHI, consistent with the requirements of Section 13405 of the HITECH Act and 45 CFR § 164.522, when the Department determines to do so (except as required by law) and if the disclosure is to a health plan for payment or health care operations and it pertains to a health care item or service for which the health care provider was paid in full "out-of-pocket."

v. Immediate Discontinuance of Use or Disclosure. The Business Associate will immediately discontinue use or disclosure of Department PHI pertaining to any individual when so requested by Department. This includes, but is not limited to, cases in which an individual has withdrawn or modified an authorization to use or disclose PHI.

g. Retention of PHI. Notwithstanding section 4.a. of this Agreement, Business Associate and its subcontractors or agents shall retain all PHI pursuant to state and federal law and shall continue to maintain the PHI required under Section 3.f. of this Agreement for a period of six (6) years after termination of the Agreement, or longer if required under state law.

h. Agent's, Subcontractor's Compliance. The Business Associate shall notify the Department of all subcontracts and agreements relating to the Agreement, where the subcontractor or agent receives PHI as described in section 2.a. of this Agreement. Such notification shall occur within 30 (thirty) calendar days of the execution of the subcontract and shall be delivered to the Department Privacy Officer. The Business Associate will ensure that any of its subcontractors, to whom it provides any of the PHI it receives hereunder, or to whom it provides any PHI which the Business Associate creates or receives on behalf of the Department, agree to the restrictions and conditions which apply to the Business Associate hereunder. The Department may request copies of downstream subcontracts and agreements to determine whether all restrictions, terms and conditions have been flowed down. Failure to ensure that downstream contracts,

subcontracts and agreements contain the required restrictions, terms and conditions may result in termination of the Agreement.

i. Federal and Department Access. The Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI, as well as the PHI, received from, or created or received by the Business Associate on behalf of the Department available to the U.S. Secretary of Health and Human Services consistent with 45 CFR § 164.504. The Business Associate shall also make these records available to Department, or Department's contractor, for periodic audit of Business Associate's compliance with the Privacy and Security Rules. Upon Department'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.

j. Security. The Business Associate shall take all steps necessary to ensure the continuous security of all PHI and data systems containing PHI. In addition, compliance 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 is required, to the extent practicable. If Business Associate chooses not to adopt such methodologies as defined in 74 FR 19006 to secure the PHI governed by this Agreement, it must submit such written rationale, including its Security Risk Analysis, to the Department Security Officer for review prior to the execution of the Agreement.

k. Notification of Breach. During the term of this Agreement, the Business Associate shall notify the Privacy Officer immediately by e-mail or web form upon the discovery of any Breach of unsecured PHI; or within 24 hours by e-mail or web form of any suspected Security Incident, intrusion or unauthorized use or disclosure of PHI in violation of this Agreement, or potential loss of confidential data affecting this Agreement. Notification shall be provided to the Department Privacy Officer.

The Business Associate shall immediately investigate such Security Incident, Breach, or unauthorized use disclosure of PHI or confidential data. Within 72 hours of the discovery, the Business Associate shall notify the Department Privacy Officer, unless otherwise directed by the Department in writing: (a) Date of discovery; (b) What data elements were involved and the extent of the data involved in the Breach; (c) A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or confidential data; (d) A description of where the PHI or confidential data is believed to have been improperly transmitted, sent, or utilized; (e) A description of the probable causes of the improper use or disclosure; and (f) Whether any federal or state laws requiring individual notifications of Breaches are triggered.

Department will coordinate with Business Associate to determine additional specific actions that will be required of the Business Associate for mitigation of the Breach, which

may include notification to the individual or other authorities.

All associated costs shall be borne by the Business Associate. This may include, but not be limited to, costs associated with notifying affected individuals.

If the Business Associate enters into a subcontract relating to the Agreement where the subcontractor or agent receives PHI as described in section 2.a. of this Agreement, all such subcontracts or downstream agreements shall contain the same incident notification requirements as contained herein, with reporting directly to the Department Privacy Officer. Failure to include such requirement in any subcontract or agreement may result in the Department's termination of the Agreement.

l. Assistance in Litigation or Administrative Proceedings. The 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 the Department at no cost to the Department to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the Department, its officers or employees based upon claimed violations of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inaction or actions by the Business Associate, except where Business Associate or its subcontractor, workforce or agent is a named as an adverse party.

4. Agreement Administration.

a. Term. This Agreement shall terminate on termination of the underlying Agreement or on the date the Department terminates for cause as authorized in paragraph (c) of this Section, whichever is sooner.

b. Duties at Termination. Upon any termination of the underlying Agreement, the Business Associate shall return or destroy, at the Department's option, all PHI created or received by the Business Associate on behalf of the Department that the Business Associate still maintains in any form and retain no copies of such PHI or, if such return or destruction is not feasible, the Business Associate shall extend the protections of this Agreement to the PHI and limit further uses and disclosures to the purposes that make the return or destruction of the PHI infeasible. This shall also apply to all agents and subcontractors of Business Associate. The duty of the Business Associate and its agents and subcontractors to assist the Department with any HIPAA required accounting of disclosures survives the termination of the underlying Agreement.

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

d. Judicial or Administrative Proceedings. The Department may terminate this

Agreement if the Business Associate is found guilty of a criminal violation of HIPAA. The Department may terminate this Agreement if the finding or stipulation that the Business Associate has violated any standard or requirement of HIPAA/HITECH, or other security or privacy laws is made in any administrative or civil proceeding in which the 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. Survival. The respective rights and obligations of Business Associate under this Agreement shall survive the termination of the underlying Agreement.

5. General Provisions/Ownership of PHI.

a. Retention of Ownership. Ownership of the PHI resides with the Department and is to be returned on demand or destroyed at the Department's option, at any time, and subject to the restrictions found within section 4. b. above.

b. Secondary PHI. Any data or PHI generated from the PHI disclosed hereunder which would permit identification of an individual must be held confidential and is also the property of Department.

c. Electronic Transmission. Except as permitted by law or this Agreement, the PHI or any data generated from the PHI which would permit identification of an individual must not be transmitted to another party by electronic or other means for additional uses or disclosures not authorized by this Agreement or to another contractor, or allied Department, or affiliate without prior written approval of Department.

d. No Sales. Reports or data containing the PHI may not be sold without Department's or the affected individual's written consent.

e. 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 Department, Business Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

f. Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules. The provisions of this Agreement shall prevail over any provisions in the underlying Agreement that may conflict or appear inconsistent with any provisions in this Agreement. The interpretation of this Agreement shall be made under the laws of the state of Alabama.

g. Amendment. The parties agree that to the extent necessary to comply with applicable law they will agree to further amend this Agreement.

h. Additional Terms and Conditions. Additional discretionary terms may be included in the release order or change order process.

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement by their duly authorized representatives to be effective as of the Date stated in the opening paragraph of this Agreement.

_____	**MOBILE COUNTY HEALTH DEPARTMENT**
SIGNED: _____	SIGNED: _____
NAME:_____	BERNARD H. EICHOLD, II, M.D., Dr. P.H., F.A.C.P
TITLE:_____	HEALTH OFFICER
DATE: _____	DATE: _____
ADDRESS: _____ _____ _____ _____	251 N. Bayou Street P. O. Box 2867 Mobile, Alabama 36652-2867
Telephone: _____	(251) 690-8827
Fax: _____	(251) 432-7443
E-Mail Address: _____ _____	beichold@mchd.org

Appendix A

Describe the **PHI** (do not include any actual PHI). **If** not applicable, please indicate the same.

Minimum PHI necessary to perform the underlying contract and may include, but is not limited to, patients' names, addresses, dates of birth, social security numbers and diagnoses.