BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (the "Agreement") is made by and between Garrett County Health Department , a unit of the Maryland Department of Health (MDH) (herein referred to as "Covered Entity") and _____ (hereinafter known as "Business Associate"). Covered Entity and Business Associate shall collectively be known herein as the "Parties."

WHEREAS, Covered Entity has a business relationship with Business Associate that is memorialized in a separate agreement (the "Underlying Agreement") dated _____ pursuant to which Business Associate may be considered a "business associate" of Covered Entity as defined in the Health Insurance Portability and Accountability Act of 1996 including all pertinent privacy regulations (45 C.F.R. Parts 160 and 164) and security regulations (45 C.F.R. Parts 160, 162, and 164), as amended from time to time, issued by the U.S. Department of Health and Human Services as either have been amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111–5), and the HIPAA Omnibus Final Rule of 2013 (collectively, "HIPAA"); and

WHEREAS, the nature of the contractual relationship between Covered Entity and Business Associate may involve the exchange of Protected Health Information ("PHI") as that term is defined under HIPAA; and

WHEREAS, for good and lawful consideration as set forth in the Underlying Agreement, Covered Entity and Business Associate enter into this Agreement for the purpose of ensuring compliance with the requirements of HIPAA and the Maryland Confidentiality of Medical Records Act (Md. Ann. Code, Health-General §§4-301 *et seq.*) ("MCMRA"); and

WHEREAS, this Agreement supersedes and replaces any and all Business Associate Agreements the Covered Entity and Business Associate may have entered into prior to the date hereof;

NOW THEREFORE, the premises having been considered and with acknowledgment of the mutual promises and of other good and valuable consideration herein contained, the Parties, intending to be legally bound, hereby agree as follows:

I. DEFINITIONS

A. Catch-all definition. The following terms used in this Agreement, whether capitalized or not, shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, 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.

B. Specific definitions:

1. Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 C.F.R. § 160.103, and in reference to the party to this Agreement, shall mean _____.

2. Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 C.F.R. § 160.103, and in reference to the party to this Agreement shall mean Garrett County Health Department.

3. HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Parts 160 and Part 164.

4. Protected Health Information ("PHI"). Protected Health Information or "PHI" shall generally have the same meaning as the term "protected health information" at 45 C.F.R. § 160.103.

II. PERMITTED USES AND DISCLOSURES OF PHI BY BUSINESS ASSOCIATE

A. Business Associate may only use or disclose PHI as necessary to perform the services set forth in the Underlying Agreement or as required by law.

B. Business Associate agrees to make uses and disclosures and requests for PHI consistent with Covered Entity's policies and procedures regarding minimum necessary use of PHI.

C. Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity.

D. Business Associate may, if directed to do so in writing by Covered Entity, create a limited data set as defined at 45 C.F.R. § 164.514(e)(2), for use in public health, research, or health care operations. Any such limited data sets shall omit any of the identifying information listed in 45 C.F.R. § 164.514(e)(2). Business Associate will enter into a valid, HIPAA-compliant Data Use Agreement as described in 45 C.F.R. § 164.514(e)(4), with the limited data set recipient. Business Associate will report any material breach or violation of the data use agreement to Covered Entity immediately after it becomes aware of any such material breach or violation.

E. Except as otherwise limited in this Agreement, Business Associate may disclose PHI for the proper management and administration or legal responsibilities of the Business Associate, provided that disclosures are Required By Law, or 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.

F. The Business Associate shall not directly or indirectly receive remuneration in exchange for any PHI of an individual pursuant to §§ 13405(d)(1) and (2) of the HITECH Act. This prohibition does not apply to the State's payment of Business Associate for its performance pursuant to the Underlying Agreement.

G. The Business Associate shall comply with the limitations on marketing and fundraising communications provided in § 13406 of the HITECH Act in connection with any PHI of individuals.

III. DUTIES OF BUSINESS ASSOCIATE RELATIVE TO PHI

A. Business Associate agrees that it will not use or disclose PHI other than as permitted or required by the Agreement, the Underlying Agreement, the MCMRA, as Required by Law, or as authorized by Covered Entity, so long as the authorized use or disclosure is permitted by law.

B. Business Associate agrees to use appropriate administrative, technical and physical safeguards to protect the privacy of PHI.

C. Business Associate agrees to use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic PHI, to prevent use or disclosure of PHI other than as provided for by the Agreement;

D.

1. Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided for by the Agreement of which it becomes aware, including Breaches of unsecured PHI as required by 45 C.F.R. § 164.410, and any Security Incident of which it becomes aware without unreasonable delay and in no case later than fifteen (15) calendar days after the use or disclosure.

2. If the use or disclosure amounts to a breach of unsecured PHI, the Business Associate shall ensure its report:

   a. Is made to Covered Entity without unreasonable delay and in no case later than fifteen (15) calendar days after the incident constituting the Breach is first known, except where a law enforcement official determines that a notification would impede a criminal investigation or cause damage to national security. For purposes of clarity for this Section III.D.1, Business Associate must notify Covered Entity of an incident involving the acquisition, access, use or disclosure of PHI in a manner not permitted under 45 C.F.R. Part E within fifteen (15) calendar days after an incident even if Business Associate has not conclusively determined within that time that the incident constitutes a Breach as defined by HIPAA;

   b. Includes the names of the Individuals whose Unsecured PHI has been, or is reasonably believed to have been, the subject of a Breach;

   c. Is in substantially the same form as **Exhibit A** hereto.

E. In addition to its obligations in Sections III.A-D, within 30 calendar days after the incident constituting the Breach is first known, Business Associate shall provide to Covered Entity a draft letter for the Covered Entity to review and approve for use in notifying the Individuals that their Unsecured PHI has been, or is reasonably believed to have been, the subject of a Breach. Approval of the letter must be in writing from the Privacy Officer for the Covered Entity or their designee. The letter shall include, to the extent possible:

1. A brief description of the incident, including the date of the Breach and the date of the discovery of the Breach, if known;

2. A description of the types of Unsecured PHI that were involved in the Breach (such as full name, Social Security number, date of birth, home address, account number, disability code, or other types of information that were involved);

3. Any steps the affected Individuals should take to protect themselves from potential harm resulting from the Breach;

4. A brief description of what the Business Associate is doing to investigate the Breach, to mitigate losses, and to protect against any further Breaches; and

5. Contact procedures for the affected Individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.

F. In the event the Breach occurs through the fault of Business Associate, Business Associate shall be responsible for notifying Individuals by sending via First Class U.S. Mail the approved letter described in Section III(E) no later than 60 calendar days after discovery of the Breach.

G. In the event the Breach occurs through the fault of Covered Entity, Covered Entity shall be responsible for notifying Individuals no later than 60 calendar days after Covered Entity receives notice of the Breach from the Business Associate.

H. In the event of any Breach, regardless of which party is responsible, Business Associate will provide, within 30 days after the discovery of the Breach, a proposed Breach Notification Report to be submitted to HHS Office of Civil Rights (OCR), as required by 45 CFR § 164.408(a).

1. Business Associate and Covered Entity, through its Privacy Officer or their designee, shall cooperate and determine which party will be responsible for filing the Breach Notification Report with OCR and Business Associate shall obtain a written acknowledgment from Covered Entity that assigns this responsibility to either Covered Entity or Business Associate.

2. If a Business Associate is assigned the responsibility of filing the Breach Notification Report with OCR, the Business Associate shall seek and receive written approval from the Covered Entity of the Breach Notification Report prior to it being filed with OCR.

3. Written approval from Covered Entity pursuant to this paragraph shall be from the MDH Privacy Officer of their designee.

I. In the event of any Breach in which 500 or more individuals of any state or jurisdiction are affected, regardless of which party is responsible, the following provisions will apply, as required by 45 CFR §164.406(a):

1. Covered Entity, through its Privacy Officer or their designee, shall determine, in consultation with Business Associate, which party will be responsible for notifying the media, and shall inform Business Associate in writing as to its determination.

2. If Business Associate is assigned the responsibility of notifying the media, Business Associate shall seek written approval from Covered Entity as to the content of any

notification to be made to the media prior to any media outlet being notified of the breach and shall incorporate any language suggested by Covered Entity.

3. If assigned responsibility, Business Associate shall provide its proposed media notification to Covered Entity for review within thirty (30) days of the date of discovery of the breach.

4. Written approval from Covered Entity pursuant to this paragraph shall be from the MDH Privacy Officer or their designee.

5. If Covered Entity assigns the responsibility to itself, it will inform Business Associate in writing as to this determination, and will offer Business Associate the opportunity to review the notification before it is disseminated.

J. To the extent permitted by the Underlying Agreement, Business Associate may use agents and subcontractors. In accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2) shall ensure that any subcontractors that create, receive, maintain, or transmit PHI 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, Business Associate must enter into Business Associate Agreements with subcontractors as required by HIPAA;

K. Business Associate agrees it will make available PHI in a designated record set to the Covered Entity, or, as directed by the Covered Entity, to an individual, as necessary to satisfy Covered Entity's obligations under 45 C.F.R.§ 164.524, including, if requested, a copy in electronic format;

L. Business Associate agrees it will make any amendment(s) to PHI in a designated record set as directed or agreed to by the Covered Entity pursuant to 45 C.F.R. § 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 C.F.R. § 164.526;

M. Business Associate agrees to maintain and make available the information required to provide an accounting of disclosures to the Covered Entity or, as directed by the Covered Entity, to an individual, as necessary to satisfy Covered Entity's obligations under 45 C.F.R.§ 164.528;

N. To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 C.F.R. Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s);

O. Business Associate agrees to make its internal practices, books, and records, including PHI, available to the Covered Entity and/or the Secretary of HHS for purposes of determining compliance with the HIPAA Rules.

P. Business Associate agrees to 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.

IV. TERM AND TERMINATION

A. Term. The Term of this Agreement shall be effective as of the effective date of the Contract entered into following the solicitation for _____, Solicitation # _____, and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or the PHI created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, in accordance with the termination provisions in this Section IV, or on the date the Covered Entity terminated for cause as authorized in paragraph (b) of this Section, whichever is sooner. If it is impossible to return or destroy all of the PHI provided by Covered Entity to Business Associate, or the PHI created or received by Business Associate on behalf of Covered Entity, Business Associate's obligations under this contract shall be ongoing with respect to that information, unless and until a separate written agreement regarding that information is entered into with Covered Entity.

B. Termination for Cause. Upon Covered Entity's knowledge of a material breach of this Agreement by Business Associate, Covered Entity shall:

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

2. Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and Covered Entity determines or reasonably believes that cure is not possible.

C. Effect of Termination.

1. Upon termination of this Agreement, for any reason, Business Associate shall return or, if agreed to by Covered Entity, destroy 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.

2. Should Business Associate make an intentional or grossly negligent Breach of PHI in violation of this Agreement or HIPAA or an intentional or grossly negligent disclosure of information protected by the MCMRA, Covered Entity shall have the right to immediately terminate any contract, other than this Agreement, then in force between the Parties, including the Underlying Agreement.

D. Survival. The obligations of Business Associate under this Section shall survive the termination of this agreement.

V. CONSIDERATION

Business Associate recognizes that the promises it has made in this Agreement shall, henceforth, be detrimentally relied upon by Covered Entity in choosing to continue or commence a business relationship with Business Associate.

VI. REMEDIES IN EVENT OF BREACH OF AGREEMENT

Business Associate hereby recognizes that irreparable harm will result to Covered Entity, and to the business of Covered Entity, in the event of breach by Business Associate of any of the covenants and assurances contained in this Agreement. As such, in the event of breach of any of the covenants and assurances contained in Sections II or III above, Covered Entity shall be entitled to enjoin and restrain Business Associate from any continued violation of Sections II or III. Furthermore, in the event of breach of Sections II or III by Business Associate, Covered Entity is entitled to reimbursement and indemnification from Business Associate for Covered Entity's reasonable attorneys' fees and expenses and costs that were reasonably incurred as a proximate result of Business Associate's breach. The remedies contained in this Section VI shall be in addition to, not in lieu of, any action for damages and/or any other remedy Covered Entity may have for breach of any part of this Agreement or the Underlying Agreement or which may be available to Covered Entity at law or in equity.

VII. MODIFICATION; AMENDMENT

This Agreement may only be modified or amended through a writing signed by the Parties and, thus, no oral modification or amendment hereof shall be permitted. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the HIPAA rules and any other applicable law.

VIII. INTERPRETATION OF THIS AGREEMENT IN RELATION TO OTHER AGREEMENTS BETWEEN THE PARTIES

Should there be any conflict between the language of this Agreement and any other contract entered into between the Parties (either previous or subsequent to the date of this Agreement), the language and provisions of this Agreement shall control and prevail unless the parties specifically refer in a subsequent written agreement to this Agreement by its title and date and specifically state that the provisions of the later written agreement shall control over this Agreement.

IX. COMPLIANCE WITH STATE LAW

The Business Associate acknowledges that by accepting the PHI from Covered Entity, it becomes a holder of medical information under the MCMRA and is subject to the provisions of that law. If the HIPAA Privacy or Security Rules and the MCMRA conflict regarding the degree of protection provided for PHI, Business Associate shall comply with the more restrictive protection requirement.

X. MISCELLANEOUS

A. Ambiguity. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy and Security Rules.

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. Agency. The Business Associate or Subcontractor is acting as an independent contractor and not as the agent of the Covered Entity or Business Associate. This Agreement does not give the Covered Entity or Business Associate such control over operational activities so as to make the

Business Associate the agent of the Covered Entity, or the Subcontractor the agent of the Business Associate.

D. No Private Cause of Action. This Agreement is not intended to and does not create a private cause of action by any individual, other than the parties to this Agreement, as a result of any claim arising out of the Breach of this Agreement, the HIPAA Standards, or other state or federal law or regulation relating to privacy or confidentiality.

E. Notice to Covered Entity. Any notice required under this Agreement to be given to Covered Entity shall be made in writing to:

Jennifer E. Hare, Administrator
Garrett County Health Department
1025 Memorial Drive
Oakland, MD 21550
Phone: (301) 334-7703

F. Notice to Business Associate. Any notice required under this Agreement to be given Business Associate shall be made in writing to:

Address: _____

_____

Attention: _____

Phone: _____

G. Survival. Any provision of this Agreement which contemplates performance or observance subsequent to any termination or expiration of this contract shall survive termination or expiration of this Agreement and continue in full force and effect.

H. Severability. If any term contained in this Agreement is held or finally determined to be invalid, illegal, or unenforceable in any respect, in whole or in part, such term shall be severed from this Agreement, and the remaining terms contained herein shall continue in full force and effect, and shall in no way be affected, prejudiced, or disturbed thereby.

I. Terms. All of the terms of this Agreement are contractual and not merely recitals and none may be amended or modified except by a writing executed by all parties hereto.

J. Priority. This Agreement supersedes and renders null and void any and all prior written or oral undertakings or agreements between the parties regarding the subject matter hereof.

IN WITNESS WHEREOF and acknowledging acceptance and agreement of the foregoing, the Parties affix their signatures hereto.

COVERED ENTITY:	**BUSINESS ASSOCIATE:**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

EXHIBIT A

FORM OF NOTIFICATION TO COVERED ENTITY OF BREACH OF UNSECURED PHI

This notification is made pursuant to Section III.2.D(2) of the Business Associate Agreement between Garrett County Health Department, a unit of the Maryland Department of Health (MDH), and _____ (Business Associate).

Business Associate hereby notifies MDH that there has been a breach of unsecured Protected Health Information (PHI) that Business Associate has used or has had access to under the terms of the Business Associate Agreement.

Incident Specific Questions:

1. Please provide a brief description of the incident, including what type of information was disclosed or accessed, who received the information and the manner in which it was accessed or disclosed. Also include the names and contact information for all individuals involved:

   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____

2. If you believe this incident was inadvertent, accidental or unintentional, please provide any information you have to support that determination:

   _____
   _____
   _____
   _____

3. Was the information viewed or actually retained by someone who should not have the information? If so, please explain:

   _____
   _____
   _____
   _____

4. What type of identifying information (e.g. names, SSN, medical record number etc.) was acquired, accessed or disclosed?

   _____
   _____

_____
_____

5. If available, please provide any information you have about the person or entity that received the information:

_____
_____
_____
_____

6. What steps, if any, have been taken to contain or mitigate the incident? Please provide as much descriptive information as possible:

_____
_____
_____
_____
_____
_____
_____

Additional Incident Details:

Date incident occurred: _____ Date incident was discovered: _____

Estimate number of individuals affected by the breach: _____

Type of incident (e.g. loss, theft, improper disposal, unauthorized access, hacking):

_____
_____

Location of information breach (e.g. laptop, desktop, email, paper files etc.):

_____
_____

Type of information involved (e.g. demographic, financial, clinical):

_____
_____

Safeguards that were in place prior to the breach (e.g. firewalls, encryptions, locks, training):

_____
_____

Please provide any other information you have or believe may be helpful in investigating or resolving this incident. If you wish to include any attachments to this form, please describe the attachments here:

_____
_____
_____
_____
_____

_____
_____
_____
_____
_____
_____
_____
_____

_____ _____

Name **Date**

_____

Signature

Please send this form by email to the GCHD Privacy Officer - jennifer.hare@maryland.gov