

**MARYLAND HEALTH BENEFIT EXCHANGE  
ATTACHMENT G - NON-EXCHANGE ENTITY AGREEMENT**

This Non-Exchange Entity Agreement (this “Agreement”) is made by and between the Maryland Health Benefit Exchange, a public corporation and independent unit of the government of the State of Maryland (“MHBE”) and \_\_\_\_\_ (the “Non-Exchange Entity” or “\_\_\_\_\_”), as of the Effective Date defined below. Each of MHBE and the Non-Exchange Entity is a “Party” to this Agreement and shall collectively be known as the “Parties”.

**RECITALS**

WHEREAS, MHBE is a state-based exchange established pursuant to the Patient Protection and Affordable Care Act of 2010 (Pub. L. 111-148) as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law No. 111-152) (together with regulations promulgated pursuant thereto, the “ACA”), and particularly pursuant to 45 C.F.R. § 155.100, as well as pursuant to Title 31 of the Insurance Article of the Maryland Code Annotated, and

WHEREAS, the Non-Exchange Entity submitted a proposal in response to that certain Maryland Health Benefit Exchange Request for Proposals: \_\_\_\_\_ [NAME OF RFP], Solicitation No. \_\_\_\_\_ (the “RFP”); and

WHEREAS, the Non-Exchange Entity has been notified of award or awarded a contract (the "Underlying Agreement") pursuant to the RFP; and

WHEREAS, the execution of this Agreement is required pursuant to the RFP, which is incorporated into the Underlying Agreement and is a part thereof; and

WHEREAS, MHBE and the Non-Exchange Entity enter into this Agreement effective as of the effective date of the Underlying Agreement (the “Effective Date”), pursuant to which the Non-Exchange Entity shall provide services to perform the functions set forth in the Underlying Agreement, as well as in any subsequent Task

Orders issued pursuant to the Underlying Agreement; and

WHEREAS, the relationship between MHBE and the Non-Exchange Entity shall involve access to Personally Identifiable Information (“PII”), as that term is defined herein, for purposes authorized under the ACA and, more particularly, under 45 C.F.R. § 155.200; and

WHEREAS, the Non-Exchange Entity’s access to PII submitted to the Exchange shall make the entity a “Non-Exchange Entity”, as that term is defined in 45 C.F.R. § 155.260(b)(1); and

WHEREAS, for good and lawful consideration as set forth in the Underlying Agreement, MHBE and the Non-Exchange Entity each acknowledge and agree that they enter into this Agreement for the purposes, among others as may be detailed herein, of ensuring the confidentiality, privacy and security of data accessed by the Non-Exchange Entity or exchanged between the Parties under this Agreement and compliance with the requirements of the ACA, including 45 C.F.R. § 155.260(b)(2) and, regardless of whether otherwise applicable to the Non-Exchange Entity, 45 C.F.R. § 155.270(a); and

WHEREAS, this Agreement supersedes and replaces any and all Business Associate Agreements, Data Use Agreements or Non-Exchange Entity Agreements the Non-Exchange Entity and MHBE may have entered into prior to the date hereof;

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

## AGREEMENT

A. **Recitals.** The Recitals are true and correct in all respects, are incorporated into this Agreement and form a part of this Agreement.

B. **Definitions.** For purposes of this Agreement, the Parties agree that the following definitions apply, regardless of whether the identified word is capitalized herein:

1. **“Breach”** shall mean the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose (as defined by OMB

Memorandum M-17-12 (Jan. 3, 2017)).

2. “Incident” means an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies (as defined by OMB Memorandum M-17-12).

3. “Personally Identifiable Information” or “PII” shall mean personally identifiable information as defined by OMB Memorandum M-17-12 (January 3, 2017) (“PII refers to information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual”).

4. “Unsecured PII” shall include, but not be limited to, electronic PII that is not encrypted by use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

C. Permitted Uses and Disclosure of PII by the Non-Exchange Entity.

1. Non-Exchange Entity may only use or disclose PII as necessary to perform the services set forth in the Underlying Agreement or as required by law.

2. Non-Exchange Entity agrees to limit uses, disclosures and requests for PII to the minimum necessary to accomplish its intended purposes.

3. Non-Exchange Entity shall not use or disclose PII in a manner that would violate 45 C.F.R. § 155.260 if done by MHBE.

4. Except as otherwise limited in this Agreement, Non-Exchange Entity agrees to disclose PII for the proper management and administration, or legal responsibilities of the Non-Exchange Entity only when (i) such disclosures are required by law, or (ii) Non-Exchange Entity obtains reasonable assurances from the person to whom the information is disclosed that the information 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 Non-Exchange Entity of any instances of which it is aware in which the confidentiality of the information has been breached.

5. Non-Exchange Entity shall not directly or indirectly receive remuneration in exchange for any PII of an individual. For the avoidance of doubt, this provision shall not preclude Non-Exchange Entity from receiving payment for the provision of services

set forth in the Underlying Agreement or that are required by law.

6. Non-Exchange Entity shall not use or disclose PII for the purposes of marketing a product or service unless necessary to perform the services set forth in the Underlying Agreement or required by law. For the purposes of this provision, “marketing” shall mean a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

**D. Duties of the Non-Exchange Entity Relative to PII.**

1. The Non-Exchange Entity shall not use or disclose PII other than as permitted or required by the Agreement or as required by law.

2. The Non-Exchange Entity shall use appropriate administrative, technical and physical safeguards to protect the privacy of PII including, without limitation, by storing electronic PII in encrypted format.

3. Non-Exchange Entity shall use privacy and security standards at least as protective as MHBE has established and implemented for itself. For example, and without limitation, Non-Exchange Entity shall comply with the standards, implementation specifications, operating rules, and code sets adopted in 45 C.F.R. Parts 160 and 162, regardless of whether otherwise made applicable to Non-Exchange Entity pursuant to 45 C.F.R. § 155.270(a), to provide for the secure exchange of PII and to prevent use or disclosure of PII other than as provided in the Agreement. Further, Non-Exchange Entity shall:

- a. **Comply with the Minimum Acceptable Risk Standards for Exchanges (MARS-E)** as published in the following suite of documents: (1) Harmonized Security and Privacy Framework – Exchange Reference Architecture Supplement; (2) Minimum Acceptable Risk Standards for Exchanges – Exchange Reference Architecture Supplement; (3) Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement; (4) ACA System Security Plan Procedures; (5) ACA System Security Plan Template; (6) ACA System Security Plan Workbook; and (7) IRS ACA Safeguard Procedures Report Template.
- b. Implement administrative, physical and technical safeguards to protect PII accessed pursuant to this Agreement and the Underlying Agreement from loss, theft or inadvertent disclosure.
- c. Safeguard PII at all times, regardless of whether or not the Non-Exchange Entity’s employee, contractor, or agent is at his or her regular duty station.
- d. Ensure that laptops and other electronic devices/media containing PII are encrypted and/or password protected.

- e. Send emails containing PII only if encrypted and being sent to and being received by email addresses of persons authorized to receive such information.
- f. Limit disclosure of the information and details relating to a PII loss only to those with a need to know.
- g. Restrict access to PII only to those authorized employees, contractors, and agents who need such data to perform their official duties in connection with purposes identified in this Agreement and the Underlying Agreement; such restrictions shall include, at a minimum, role-based access that limits access to those individuals who need it to perform their official duties in connection with the uses of data authorized in this Agreement and the Underlying Agreement (“authorized users”). Further, the Non-Exchange Entity shall advise all users who will have access to the data provided under this Agreement and the Underlying Agreement of the confidential nature of the data, the safeguards required to protect the data, and the civil and criminal sanctions for noncompliance contained in the applicable State and federal laws.

4. Non-Exchange Entity shall monitor, periodically assess, and update its security controls and related system risks, to ensure the continued effectiveness of those controls.

5. Non-Exchange Entity shall inform MHBE of any change in its administrative, technical or operational environments to the extent any are material in the Underlying Agreement.

6. Non-Exchange Entity shall require any agents or downstream entities to which access to PII is granted in connection with the Underlying Agreement to adhere to the same privacy and security standards and obligations to which Non-Exchange Entity hereby agrees.

7. Non-Exchange Entity shall report to MHBE any use or disclosure of PII not permitted by this Agreement or required by law, including any Breaches of PII of which it becomes aware. Non-Exchange Entity further agrees to report to MHBE any Incident of which it becomes aware without unreasonable delay, and in no case later than five (5) calendar days after the Incident. Further, Non-Exchange Entity shall report all suspected or confirmed Incidents involving loss or suspected loss of PII to MHBE within *one* (1) hour of discovery.

8. If the use or disclosure amounts to a Breach of Unsecured PII, the Non-Exchange Entity shall ensure its report:

- a. Is made to MHBE 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 the avoidance of doubt, Non-Exchange Entity must notify MHBE of an incident involving the acquisition, access, use or disclosure of PII in a manner not permitted under 45 C.F.R. § 155.260 or this Agreement within five (5) calendar days after an Incident even if Non-Exchange Entity has not conclusively determined within that time that the Incident constitutes a Breach as defined by this Agreement;

b. Includes the names of the individuals whose unsecured PII has been, or is reasonably believed to have been, the subject of a Breach;

c. Is in substantially the same form as **EXHIBIT 1** attached hereto; and

d. Includes a draft letter for MHBE to review and approve prior to Non-Exchange Entity's notification of the affected individuals that their unsecured PII has been, or is reasonably believed to have been, the subject of a Breach. The notification must include, to the extent possible:

i) A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

ii) The types of Unsecured PII that were involved in the Breach (such as full name, Social Security number, date of birth, home address, account number, or other types of information that were involved);

iii) Any steps the affected individuals should take to protect themselves from potential harm resulting from the Breach;

iv) The toll-free telephone numbers and addresses for the major consumer reporting agencies;

v) The toll-free telephone numbers, addresses and web site addresses for (1) the Federal Trade Commission; and (2) the Maryland Office of the Attorney General;

vi) A brief description of what MHBE and the Non-Exchange Entity are doing to investigate the Breach, to mitigate losses, and to protect against any further Breaches; and

- vii) Contact procedures for the affected individuals to ask questions or learn additional information, which shall include a telephone number, toll-free telephone number if one is maintained and postal address and may include an email address and web-site address.

9. To the extent permitted by the Underlying Agreement, Non-Exchange Entity may use agents and subcontractors. The Non-Exchange Entity shall ensure that any subcontractors or agents that create, receive, maintain, or transmit PII on behalf of Non-Exchange Entity agree to the same restrictions, conditions and requirements that apply to Non-Exchange Entity with respect to such information.

10. Non-Exchange Entity agrees to maintain and make available the information required to prove an accounting of disclosures of PII to MHBE or, as directed by MHBE, to an individual.

11. Non-Exchange Entity agrees to make its internal practices, books, and records, including PII, available to MHBE and/or the Secretary of the U.S. Department of Health and Human Services for purposes of determining compliance with the ACA's privacy and security regulations as well as with the standards MHBE has established pursuant to 45 C.F.R. § 155.260, as set forth in 45 C.F.R. § 155.280(a).

12. Non-Exchange Entity agrees to mitigate, to the extent practicable, any harmful effect known to Non-Exchange Entity of a use or disclosure of PII by Non-Exchange Entity in violation of the requirements of this Agreement.

#### E. Term and Termination.

1. Term. The Term of this Agreement shall be effective as of the Effective Date defined above and shall terminate when all of the PII provided by MHBE to the Non-Exchange Entity, or the PII created or received by Non-Exchange Entity on behalf of MHBE, is destroyed or returned to MHBE, in accordance with the termination provisions in this Section E, or on the date MHBE terminates for cause as authorized in paragraph (2) of this Section, whichever is sooner. If it is impossible to return or destroy all of the PII provided by MHBE to Non-Exchange Entity, or the PII created or received by Non-Exchange Entity on behalf of MHBE, Non-Exchange Entity'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 MHBE.

2. Termination. Upon MHBE's knowledge of a material breach of this

Agreement by Non- Exchange Entity, MHBE:

- a. Shall provide an opportunity for Non-Exchange Entity to cure the breach or end the violation and, if Non-Exchange Entity does not cure the breach or end the violation within the time specified by MHBE, may terminate this Agreement; or
- b. May immediately terminate this Agreement if Non-Exchange Entity has breached a material term of this Agreement and MHBE determines or reasonably believes that cure is not possible.

3. Effect of Termination.

a. Upon termination of this Agreement, for any reason, Non-Exchange Entity shall return or, if agreed to by MHBE, destroy all PII received from MHBE, or created, maintained, or received by Non-Exchange Entity on behalf of MHBE, which the Non-Exchange Entity maintains in any form. Non-Exchange Entity shall retain no copies of the PII. This provision shall apply to PII that is in the possession of subcontractors or agents of Non-Exchange Entity.

b. Should Non-Exchange Entity make an intentional or grossly negligent Breach of PII in violation of this Agreement or applicable law, MHBE shall have the right to immediately terminate any contract, other than this Agreement, then in force between the Parties, as well as the Underlying Agreement.

4. Survival. The obligations of Non-Exchange Entity under this Section shall survive the termination of this Agreement.

F. **Consideration.** Non-Exchange Entity recognizes that the promises it has made in this Agreement shall, henceforth, be detrimentally relied upon by MHBE in choosing to continue or commence a business relationship with Non-Exchange Entity.

G. **Remedies in the Event of Breach.** Non-Exchange Entity hereby recognizes that irreparable harm will result to MHBE, and to the business of MHBE, in the event of breach by Non- Exchange Entity 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 C or D above, MHBE shall be entitled to enjoin and restrain Non-Exchange Entity from any continued violation of Sections C or D. Furthermore, in the event of breach of Sections C or D by Non-Exchange Entity, MHBE is entitled to reimbursement and indemnification from Non-Exchange Entity for MHBE's reasonable attorneys' fees and expenses and costs that were reasonably incurred as a proximate result of Non-Exchange Entity's breach. The remedies contained in this Section G shall be in addition to, not in lieu of, any action for damages and/or any other remedy MHBE may have for breach of any part of this Agreement or

the Underlying Agreement or which may be available to MHBE at law or in equity.

H. **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 MHBE to comply with the requirements of the ACA and, were it to become or imminently be applicable, the Health Insurance Portability and Accountability Act of 1996, as amended, together with all regulations promulgated thereto, and any other applicable law.

I. **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.

J. **Governing Law.** This Agreement shall be governed and construed in accordance with the laws of the State of Maryland, including, without limitation, Title 12 of the State Government Article of the Annotated Code of Maryland, but without regard to its choice of law provisions. This Agreement is not intended to modify the Parties' respective obligations to comply with all applicable federal, state and local laws, rules, and regulations, including but in no way limited to any and all laws, rules, and regulations related to privacy protection and confidentiality.

K. **Miscellaneous.**

1. **Ambiguity.** Any ambiguity in this Agreement shall be resolved to permit MHBE to comply with the ACA and its provisions with respect to the privacy and security of personally identifiable information.

2. **Regulatory References.** A reference in this Agreement to a section in the ACA, including any regulations promulgated thereto, means the section as in effect or as amended.

3. **Notice to MHBE.** Any notice required under this Agreement to MHBE shall be made in writing to:

Caterina Pañgilinan  
Chief Compliance Officer  
Maryland Health Benefit Exchange  
750 E. Pratt Street, 6<sup>th</sup> Floor  
Baltimore, MD 21202  
Phone: (410) 547-1838  
Email: [caterina.pangilinan@maryland.gov](mailto:caterina.pangilinan@maryland.gov)

With a copy to:  
Sharon S. Street, Principal ounsel  
Office of the Attorney General  
Maryland Health Benefit Exchange  
750 E. Pratt Street, 6<sup>th</sup> Floor  
Baltimore, MD 21202  
Phone: (410) 547-7378  
Email: [sharon.street1@maryland.gov](mailto:sharon.street1@maryland.gov)

4. Notice to Non-Exchange Entity. Any notice required under this Agreement to be given Non-Exchange Entity shall be made in writing to:

Address: \_\_\_\_\_

Attention: \_\_\_\_\_

Phone: \_\_\_\_\_

Email: \_\_\_\_\_

5. Method of Notice. Notices shall be sufficient if made by email and acknowledged within 24 hours by reply email, or delivered by a nationally recognized overnight carrier, such as FedEx, or via U.S. Mail-Certified Delivery, Return Receipt Requested.

6. Notice of Legal Requests. Non-Exchange Entity shall give notice to MHBE upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the MHBE's data under this Agreement, or which in any way might reasonably require access to the data of the MHBE, unless prohibited by law from providing such notice. The Non-Exchange Entity shall not respond to subpoenas, service of process and other legal requests related to MHBE without first notifying the MHBE, unless prohibited by law from providing such notice.

7. 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.

8. 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.

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

10. 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.

[Signatures on next page(s)]

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

**MHBE:**

**NON-EXCHANGE ENTITY:**

By: \_\_\_\_\_

By: \_\_\_\_\_

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_

Approved as to form and legal sufficiency this \_\_\_\_\_ day of \_\_\_\_\_, 2020.

By: \_\_\_\_\_  
Assistant Attorney General  
Maryland Health Benefit  
Exchange

**ATTACHMENT G - EXHIBIT 1  
[IRS SAFEGUARDING CONTRACT LANGUAGE]**

**I. PERFORMANCE**

In performance of the Underlying Agreement, the Non-Exchange Entity (hereinafter, "Contractor") agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be done under the supervision of the Contractor or the Contractor's employees.

(2) The Contractor and the Contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.

(3) Any return or return information (as each is respectively defined in 26 U.S.C. § 6103(b)(1)-(b)(2), hereafter referred to as "return(s)" or "return information") made available in any format shall be used only for the purpose of carrying out the provisions of the Underlying Agreement. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of the Underlying Agreement. Disclosure to anyone other than an officer or employee of the Contractor will be prohibited.

(4) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.

(5) The Contractor certifies that the data processed during the performance of the Underlying Agreement will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the Contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

(6) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the MHBE or his or her designee. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.

(7) All computer systems receiving, processing, storing or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be

available and activated to protect against unauthorized use of and access to Federal Tax Information.

(8) No work involving Federal Tax Information furnished under the Underlying Agreement will be subcontracted without prior written approval of the MHBE and the IRS.

(9) The Contractor will maintain a list of employees authorized access. Such list will be provided to the MHBE and, upon request, to the IRS reviewing office.

(10) The MHBE will have the right to void the Underlying Agreement if the Contractor fails to provide the safeguards described above.

## **II. CRIMINAL/CIVIL SANCTIONS**

(1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by 26 U.S.C. §§ 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

(2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of the Underlying Agreement. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the Underlying Agreement. Inspection by or disclosure to anyone without an official need-to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs

of the action. These penalties are prescribed by 26 U.S.C. §§ 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(3) Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed 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 [MHBE] 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 the 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.

(4) Granting a Contractor access to FTI must be preceded by certifying that each individual understands the MHBE's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the MHBE's files for review. As part of the certification and at least annually afterwards, Contractors must be advised of the provisions of 26 U.S.C. §§ 7431, 7213, and 7213A (see IRS Publication 1075 Exhibit 4, Sanctions for Unauthorized Disclosure, and IRS Publication 1075 Exhibit 5, Civil Damages for Unauthorized Disclosure). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See IRS Publication 1075 Section 10). For both the initial certification and the annual certification, the Contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

### **III. INSPECTION**

Each of the IRS and the MHBE, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the Contractor to inspect facilities and operations performing any work with FTI under the Underlying Agreement for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the Contractor is found to be noncompliant with Underlying Agreement safeguards.



ATTACHMENT G - EXHIBIT 2

EXHIBIT 1 TO THE NON-EXCHANGE ENTITY AGREEMENT
MHBE NOTIFICATION OF ACTUAL OR POTENTIAL
PRIVACY – IT SECURITY INCIDENT REPORT

Date Reported to MHBE: \_\_\_\_\_

This notification is made pursuant to the Non-Exchange Entity Agreement between the MARYLAND HEALTH BENEFIT EXCHANGE, a public corporation and independent unit of State government ("MHBE") and reporting agency \_\_\_\_\_ ("Insert Non-Exchange Entity name"). Non-Exchange Entity hereby notifies MHBE that there has been an actual or potential breach of unsecured personally identifiable information ("PII") that Non-Exchange Entity has used or has had access to under the terms of the Non-Exchange Entity Agreement. Please provide as much detail as possible.

1) Description of the breach:

Four horizontal lines for describing the breach.

2) Were documents inappropriately loaded into wrong account? [ ] Yes [ ] No

If "yes," in wrong account, Full Name of Account Owner Application ID Document ID(s)

Form for account owner name: (First) (Middle) (Last) \_\_\_\_\_

3) Was breach identified from work list or in application while assisting a customer? [ ] Yes [ ] No

4) Date of discovery of the breach: \_\_\_\_\_ Date of the breach: \_\_\_\_\_

5) Does the breach involve 500 or more individuals? Yes/No

6) Number of individuals "affected" (read: Number whose PII was exposed) by the breach: \_\_\_\_\_

7) Name(s) of individuals "affected" by the breach (read: whose PII was expose): (attach list if over 5)

.1 \_\_\_\_\_ Application ID \_\_\_\_\_

(Please Complete Other Side)

.2 \_\_\_\_\_ Application ID \_\_\_\_\_

.3 \_\_\_\_\_ Application ID \_\_\_\_\_

.4 \_\_\_\_\_ Application ID \_\_\_\_\_

.5 \_\_\_\_\_ Application ID \_\_\_\_\_

8) For each “affected” individual, explicitly list the types of unsecured PII that were involved in the breach (such as “full name”, “Social Security number”, “date of birth”, “Medicaid number”, “home address”, “account number”, “passport number,” or other number.. *(Please refrain from simply identifying the type of document)*):

	Name(s) of “Affected” Party	Document ID #	Types of PII
.1	_____	_____	_____
.2	_____	_____	_____
.3	_____	_____	_____
.4	_____	_____	_____
.5	_____	_____	_____

9) Was breach caused by reporting entity?     Yes             No

If “yes,” Description of what Non-Exchange Entity is doing to investigate the breach, to mitigate losses, and to protect against any further breaches:

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

10) Contact information to ask questions or learn additional information:

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Address: \_\_\_\_\_

\_\_\_\_\_

Email Address: \_\_\_\_\_



Phone Number: \_\_\_\_\_

Please securely email completed form to [mhbeincident.report@maryland.gov](mailto:mhbeincident.report@maryland.gov) or call Cat Pañgilinan, MHBE Chief Compliance Officer, at 410-547-1838, if you have any questions.

Thank You!

(FORM) MHBE Notification of Privacy-IT Security Incident Report 2019-04-15