APPENDIX A

PRIVACY AND SECURITY STANDARDS AND IMPLEMENTATION SPECIFICATIONS FOR NON-EXCHANGE ENTITIES

Statement of Applicability:

These standards and implementation specifications are established in accordance with Section 1411(g) of the Affordable Care Act (42 U.S.C. § 18081(g)) and 45 CFR 155.260. As used in this document, all terms used herein carry the meanings assigned in Appendix B, attached to this Agreement.

The standards and implementation specifications that are set forth in this Appendix A and Version 1.0 of the Minimum Acceptable Risk Standards—Exchanges (MARS-E) suite of documents (which can be found at http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/) are the same as, or more stringent than, the privacy and security standards and implementation specifications that the Centers for Medicare and Medicaid Services ("CMS") has established for the Federally-Facilitated Exchanges ("FFEs") established under Section 1321(c) of the Affordable Care Act (42 U.S.C. § 18041(c)).

CMS will enter into contractual agreements with Non-Exchange Entities that gain access to Personally Identifiable Information ("PII") exchanged with the FFEs, or directly from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, or these individuals' legal representative(s) or Authorized Representative(s). Each such agreement and its appendices, which include this Appendix A, govern any PII that is created, collected, disclosed, accessed, maintained, stored, or used by the Non-Exchange Entity in the context of the FFE.

Organizations designated by CMS, which manages and oversees the FFEs, to certify staff members or volunteers to act as certified application counselors pursuant to 45 CFR 155.225 ("Certified Application Counselor Designated Organizations," or "CDOs") are Non-Exchange Entities and must sign a contractual agreement into which this Appendix A has been incorporated, through which they agree to comply with the standards and implementation specifications laid out in this document and the referenced MARS-E suite of documents while performing the Authorized Functions outlined in their agreement with CMS. Pursuant to 45 CFR 155.225(d)(3), and separately, pursuant to the CDO's agreement with CMS, all staff and volunteers of CDOs that are certified as certified application counselors must enter into an agreement with the CDO, in which they also agree to comply with the standards set forth in this Appendix A and the referenced MARS-E suite of documents, while performing the Authorized Functions outlined in their agreement with the CDO.

NON-EXCHANGE ENTITY PRIVACY AND SECURITY STANDARDS AND IMPLEMENTATION SPECIFICATIONS

In addition to the standards and implementation specifications set forth in the MARS-E suite of documents noted above, Non-Exchange Entities must meet the following privacy and security standards and implementation specifications to the extent they are not inconsistent with any applicable MARS-E standards.

(1) *Individual Access to PII: In keeping with the standards and implementation specifications used by the FFE, Non-Exchange Entities that maintain and/or store PII must provide Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, and/or these individuals' legal representative(s) and Authorized Representative(s), with a simple and timely means of appropriately accessing PII pertaining to them and/or the person they represent in a physical or electronic readable form and format.*

a. Standard: Non-Exchange Entities that maintain and/or store PII must implement policies and procedures that provide access to PII upon request.

i. Implementation Specifications:

1. Access rights must apply to any PII that is created, collected, disclosed, accessed, maintained, stored, and used by the Non-Exchange Entity to perform any of the Authorized Functions outlined in their respective agreements with the FFE.

2. The release of electronic documents containing PII through any electronic means of communication (e.g., e-mail, web portal) must meet the verification requirements for the release of "written documents" in Section (5)b below.

3. Persons legally authorized to act on behalf of the Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers regarding their PII, including individuals acting under an appropriate power of attorney that complies with applicable state and federal law, must be granted access in accordance with their legal authority. Such access would generally be expected to be coextensive with the degree of access available to the Subject Individual.

4. At the time the request is made, the Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employees, Qualified Employers and/or these individuals' legal representative(s) or Authorized Representative(s) should generally be required to specify which PII he or she would like access to. The Non- Exchange Entity may assist

them in determining their Information or data needs if such assistance is requested.

5. Subject to paragraphs (1)a.i.6 and 7 below, Non-Exchange Entities generally must provide access to the PII in the form or format requested, if it is readily producible in such form or format.

6. Unless the Non-Exchange Entity is a Certified Application Counselor Designated Organization or Certified Application Counselor, it may charge a fee only to recoup its costs for labor for copying the PII, supplies for creating a paper copy or a copy on electronic media, postage if the PII is mailed, or any costs for preparing an explanation or summary of the PII if the recipients has requested and/or agreed to receive such summary. If such fees are paid, the Non-Exchange Entity must provide the requested copies in accordance with any other applicable standards and implementation specifications. Under no circumstances may Certified Application Counselor Designated Organizations or Certified Application Counselors charge any consumers any fees for application or other assistance related to the Exchange

7. A Non-Exchange Entity that receives a request for notification of, or access to PII must verify the requestor's identity in accordance with Section (5)b below.

8. A Non-Exchange Entity must complete its review of a request for access or notification (and grant or deny said notification and/or access) within 30 Days of receipt of the notification and/or access request.

9. Except as otherwise provided in (1)a.i.10, if the requested PII cannot be produced, the Non-Exchange Entity must provide an explanation for its denial of the notification or access request, and, if applicable, information regarding the availability of any appeal procedures, including the appropriate appeal authority's name, title, and contact information.

10. Unreviewable grounds for denial. Non-Exchange Entities may deny access to PII that they maintain or store without providing an opportunity for review, in the following circumstances:
    a. If the PII was obtained or created solely for use in legal proceedings;
    b. If the PII is contained in records that are subject to a law that either permits withholding the PII or bars the release of such PII.

(2) *Openness and Transparency. In keeping with the standards and implementation specifications used by the FFE, Non-Exchange Entities must ensure openness and transparency about policies, procedures, and technologies that directly affect Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employers, and Qualified Employees, and/or these individuals' legal representative(s) or Authorized Representative(s), and their PII.*

a. Standard: Privacy Notice Statement. Prior to collecting PII, the Non-Exchange Entity must provide a notice that is prominently and conspicuously displayed on a public facing Web site, if applicable, or on the electronic and/or paper form the Non-Exchange Entity will use to gather and/or request PII.

i. Implementation Specifications.

1. The statement must be written in plain language and provided in a manner that is accessible and timely to people living with disabilities and with limited English proficiency.

2. The statement must contain at a minimum the following information:

a. Legal authority to collect PII;

b. Purpose of the information collection;

c. To whom PII might be disclosed, and for what purposes;

d. Authorized uses and disclosures of any collected information;

e. Whether the request to collect PII is voluntary or mandatory under the applicable law;

f. Effects of non-disclosure if an individual chooses not to provide the requested information.

3. The Non-Exchange Entity shall maintain its Privacy Notice Statement content by reviewing and revising as necessary on an annual basis, at a minimum, and before or as soon as possible after any change to its privacy policies and procedures.

4. If the Non-Exchange Entity operates a Web site, it shall ensure that descriptions of its privacy and security practices, and information on how to file complaints with CMS and the Non-Exchange Entity, are publicly available through its Web site.

(3) *Individual choice. In keeping with the standards and implementation specifications used by the FFE, Non-Exchange Entities should ensure that Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, or these individuals' legal representative(s) or Authorized Representative(s), are provided a reasonable opportunity and capability to make informed decisions about the creation, collection, disclosure, access, maintenance, storage, and use of their PII.*

a. Standard: Informed Consent. The Non-Exchange Entity may create, collect, disclose, access, maintain, store, and use PII from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, Qualified Employers or these individuals' legal representative(s) or Authorized Representative(s), only for the functions and purposes listed in the Privacy Notice Statement and any relevant agreements in effect as of the time the information is collected, unless the FFE or Non-Exchange Entity obtains informed consent from such individuals.

i. Implementation specifications:

1. The Non-Exchange Entity must obtain informed consent from individuals for any use or disclosure of information that is not permissible within the scope of the Privacy Notice Statement and any relevant agreements that were in effect as of the time the PII was collected. Such consent must be subject to a right of revocation.

2. Any such consent that serves as the basis of a use or disclosure must:

a. Be provided in specific terms and in plain language;

b. Identify the entity collecting or using the PII, and/or making the disclosure;

c. Identify the specific collections, use(s), and disclosure(s) of specified PII with respect to a specific recipient(s);

d. Provide notice of an individual's ability to revoke the consent at any time.

3. Consent documents must be appropriately secured and retained for 10 years.

(4) *Creation, collection, disclosure, access, maintenance, storage, and use limitations. In keeping with the standards and implementation specifications used by the FFE, Non-Exchange Entities must ensure that PII is only created, collected, disclosed, accessed, maintained, stored, and used, to the extent necessary to accomplish a specified purpose(s) in the contractual agreement and any appendices. Such information shall never be used to discriminate against a Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee, Qualified Employer, and/or these individuals' legal representative(s) or Authorized Representative(s).*

a. Standard: Other than in accordance with the consent procedures outlined above, the Non-Exchange Entity shall only create, collect, disclose, access, maintain, store, and use PII:

1. To the extent necessary to ensure the efficient operation of the Exchange;

2. In accordance with its published Privacy Notice Statement and any applicable agreements that were in effect at the time the PII was collected, including the consent procedures outlined above in Section (3) above; and/or

3. In accordance with the permissible functions outlined in the regulations and agreements between CMS and the Non-Exchange Entity.

b. Standard: Non-discrimination. The Non-Exchange Entity should, to the greatest extent practicable, collect PII directly from the Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee, or Qualified Employer when the information may result in adverse determinations about benefits.

c. Standard: Prohibited uses and disclosures of PII

i. Implementation Specifications:

1. The Non-Exchange Entity shall not request Information regarding citizenship, status as a national, or immigration status for an individual who is not seeking coverage for himself or herself on any application.

2. The Non-Exchange Entity shall not require an individual who is not seeking coverage for himself or herself to provide a social security number (SSN), except if an Applicant's eligibility is reliant on a tax filer's tax return and their SSN is relevant to verification of household income and family size.

3. The Non-Exchange Entity shall not use PII to discriminate, including employing marketing practices or benefit designs that will have the effect of discouraging the enrollment of individuals with significant health needs in Qualified Health Plans ("QHPs").

(5) *Data quality and integrity. In keeping with the standards and implementation specifications used by the FFE, Non-Exchange Entities should take reasonable steps to ensure that PII is complete, accurate, and up-to-date to the extent such data is necessary for the Non-Exchange Entity's intended use of such data, and that such data has not been altered or destroyed in an unauthorized manner, thereby ensuring the confidentiality, integrity, and availability of PII.*

a. Standard: Right to Amend, Correct, Substitute, or Delete PII. In keeping with the standards and implementation specifications used by the FFE, Non-Exchange Entities must offer Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, or these individuals' legal

representative(s) or Authorized Representative(s), an opportunity to request amendment, correction, substitution, or deletion of PII maintained and/or stored by the Non-Exchange Entity if such individual believes that the PII is not accurate, timely, complete, relevant, or necessary to accomplish an Exchange-related function, except where the Information questioned originated from other sources, in which case the individual should contact the originating source.

i. Implementation Specifications:

1. Such individuals shall be provided with instructions as to how they should address their requests to the Non-Exchange Entity's Responsible Official, in writing or telephonically. They may also be offered an opportunity to meet with such individual or their delegate(s) in person.

2. Such individuals shall be instructed to specify the following in each request:

a. The PII they wish to correct, amend, substitute or delete;

b. The reasons for requesting such correction, amendment, substitution, or deletion, along with any supporting justification or evidence.

3. Such requests must be granted or denied within no more than 10 working days of receipt.

4. If the Responsible Official (or their delegate) reviews these materials and ultimately agrees that the identified PII is not accurate, timely, complete, relevant or necessary to accomplish the function for which the PII was obtained/provided, the PII should be corrected, amended, substituted, or deleted in accordance with applicable law.

5. If the Responsible Official (or their delegate) reviews these materials and ultimately does not agree that the PII should be corrected, amended, substituted, or deleted, the requestor shall be informed in writing of the denial, and, if applicable, the availability of any appeal procedures. If available, the notification must identify the appropriate appeal authority including that authority's name, title, and contact information.

b. Standard: Verification of Identity for Requests to Amend, Correct, Substitute or Delete PII. In keeping with the standards and implementation specifications used by the FFE, Non-Exchange Entities that maintain and/or store PII must develop and implement policies and procedures to verify the identity of any person who requests access to; notification of; or amendment, correction, substitution, or deletion of PII that is maintained by or for the Non-Exchange Entity. This includes confirmation of an individuals' legal or personal authority to

access; receive notification of; or seek amendment, correction, substitution, or deletion of a Consumer's, Applicant's, Qualified Individuals', Enrollee's, Qualified Employee's, or Qualified Employer's PII.

i. Implementation Specifications:

1. The requester must submit through mail, via an electronic upload process, or in-person to the Non-Exchange Entity's Responsible Official, a copy of one of the following government-issued identification: a driver's license, school identification card, voter registration card, U.S. military card or draft record, identification card issued by the federal, state or local government, including a U.S. passport, military dependent's identification card, Native American tribal document, or U.S. Coast Guard Merchant Mariner card.

2. If such requester cannot provide a copy of one of these documents, he or she can submit two of the following documents that corroborate one another: a birth certificate, Social Security card, marriage certificate, divorce decree, employer identification card, high school or college diploma, and/or property deed or title.

c. Standard: Accounting for Disclosures. Except for those disclosures made to the Non-Exchange Entity's Workforce who have a need for the record in the performance of their duties; and the disclosures that are necessary to carry out the required functions of the Non-Exchange Entity, Non-Exchange Entities that maintain and/or store PII shall maintain an accounting of any and all disclosures.

i. Implementation Specifications:

1. The accounting shall contain the date, nature, and purpose of such disclosures, and the name and address of the person or agency to whom the disclosure is made

2. The accounting shall be retained for at least 10 years after the disclosure, or the life of the record, whichever is longer.

3. Notwithstanding exceptions in Section (1)a.10, this accounting shall be available to Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, Qualified Employers, and/or these individuals' legal representative(s) or Authorized Representative(s), on their request per the procedures outlined under the access standards in Section (1) above.

(6) *Accountability. In keeping with the standards and implementation specifications used by the FEE, Non-Exchange Entities should adopt and implement the standards and implementation specifications in this document and the cited MARS-E document suite, in a manner that ensures appropriate monitoring and other means and methods to identify and report Incidents and/or Breaches.*

a. Standard: Reporting. The Non-Exchange Entity must implement Breach and Incident handling procedures that are consistent with CMS' Incident and Breach Notification Procedures[1] and memorialized in the Non-Exchange Entity's own written policies and procedures. Such policies and procedures would:

i. Identify the Non-Exchange Entity's Designated Privacy Official, if applicable, and/or identify other personnel authorized to access PII and responsible for reporting and managing Incidents or Breaches to CMS.

ii. Provide details regarding the identification, response, recovery, and follow-up of Incidents and Breaches, which should include information regarding the potential need for CMS to immediately suspend or revoke access to the Hub for containment purposes; and

iii. Require reporting any Incident or Breach of PII to the CMS IT Service Desk by telephone at (410) 786-2580 or 1-800-562-1963 or via email notification at cms_it_service_desk@cms.hhs.gov within required time frames.

b. Standard: Standard Operating Procedures. The Non-Exchange Entity shall incorporate privacy and security standards and implementation specifications, where appropriate, in its standard operating procedures that are associated with functions involving the creation, collection, disclosure, access, maintenance, storage, or use of PII.

i. Implementation Specifications:

1. The privacy and security standards and implementation specifications shall be written in plain language and shall be available to all of the Non-Exchange Entity's Workforce members whose responsibilities entail the creation, collection, maintenance, storage, access, or use of PII.

2. The procedures shall ensure the Non-Exchange Entity's cooperation with CMS in resolving any Incident or Breach, including (if requested by CMS) the return or destruction of any PII files it received under the Agreement; the provision of a formal response to an allegation of unauthorized PII use, reuse or

---

1 Available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VIII_7-1_Incident_Handling_Standard.pdf 10

disclosure; and/or the submission of a corrective action plan with steps designed to prevent any future unauthorized uses, reuses or disclosures.

3. The standard operating procedures must be designed and implemented to ensure the Non-Exchange Entity and its Workforce comply with the standards and implementation specifications contained herein, and must be reasonably designed, taking into account the size and the type of activities that relate to PII undertaken by the Non-Exchange Entity, to ensure such compliance.

a. Standard: Training and Awareness. The Non-Exchange Entity shall develop training and awareness programs for members of its Workforce that create, collect, disclose, access, maintain, store, and use PII while carrying out any Authorized Functions.

i. Implementation Specifications:

1. The Non-Exchange Entity must require such individuals to successfully complete privacy and security training, as appropriate for their work duties and level of exposure to PII, prior to when they assume responsibility for/have access to PII.

2. The Non-Exchange Entity must require periodic role-based training on an annual basis, at a minimum.

3. The successful completion by such individuals of applicable training programs, curricula, and examinations offered through the FFE is sufficient to satisfy the requirements of this paragraph.

b. Standard: Security Controls. The FFE shall adopt and implement the Security Control standards cited in the MARS-E document suite for protecting the confidentiality, integrity, and availability of PII.

i. Implementation Specifications:

1. Implementation specifications for each Security Control are provided in the MARS-E document suite.