AGREEMENT BETWEEN AGENT OR BROKER AND THE CENTERS FOR MEDICARE & MEDICAID SERVICES FOR INDIVIDUAL MARKET FEDERALLY-FACILITATED EXCHANGES AND THE STATE-BASED EXCHANGES ON THE FEDERAL PLATFORM

THIS AGREEMENT ("Agreement") is entered into by and between THE CENTERS FOR MEDICARE & MEDICAID SERVICES ("CMS"), as the Party (as defined below) responsible for the management and oversight of the Federally-facilitated Exchanges* ("FFEs"), and the use of the Federal eligibility and enrollment platform by the State-based Exchanges on the Federal Platform** (SBE-FPs), including the CMS Data Services Hub ("Hub"), and the Agent, Broker, or entity who established this account and whose name appears on the Marketplace Learning Management System (MLMS) account (hereinafter referred to as "ABE"), and who, among other things, assists Consumers, Applicants, Qualified Individuals and Enrollees in applying for Advance Payments of the Premium Tax Credit ("APTC") and Cost-sharing Reductions ("CSRs") for Qualified Health Plans ("QHPs"), and/or in completing enrollment in QHPs offered in the individual market through an FFE or SBE-FP, and provides Customer Service (CMS and ABE hereinafter referred to as "Party", or collectively, as the "Parties").

** References to the Federally-facilitated Exchanges equate to the Federally-facilitated Marketplaces.*

*** References to the State-based Exchanges on the Federal Platform equate to the State-based Marketplaces on the Federal platform.*

WHEREAS:

1. Section 1312(e) of the Patient Protection and Affordable Care Act ("PPACA") provides that the Secretary of the U.S. Department of Health and Human Services ("HHS") shall establish procedures that permit Agents and Brokers to enroll Qualified Individuals in QHPs through an Exchange, and to assist individuals in applying for APTC and CSRs, to the extent allowed by States. To participate in an FFE or SBE-FP, Agents and Brokers must complete all necessary registration and training requirements under 45 CFR 155.220.

2. To facilitate the operation of the FFEs and SBE-FPs, CMS desires to permit ABE to create, collect, disclose, access, maintain, store, or use the Personally Identifiable Information ("PII") from CMS, Consumers, Applicants, Qualified Individuals, and Enrollees, or their legal representative or Authorized Representative, to the extent that these activities are necessary to carry out the Authorized Functions that the PPACA and implementing regulations permit.

3. ABE is an entity or individual licensed by the applicable State Department of Insurance ("DOI") in at least one FFE or SBE-FP state who desires to create, collect, disclose, access, maintain, store, and use PII from CMS, Consumers, Applicants, Qualified Individuals, and Enrollees to perform the Authorized Functions described in Section II.a of this Agreement.

4. 45 CFR 155.260(b) provides that an Exchange must, among other things, require privacy and security standards that are consistent with the principles in 45 CFR 155.260(a)(1) through (a)(6) and with 45 CFR 155.260(b)(3), as a condition of contract or agreement with Non-Exchange Entities, and ABE is a Non-Exchange Entity.

5. CMS, in the administration of the FFEs and the Hub, as well as the Federal eligibility and enrollment platform relied upon by SBE-FPs, has adopted privacy and security standards concerning PII, as set forth in Appendix A, "Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities."

Now, therefore, in consideration of the promises and covenants herein contained, the adequacy of which the Parties acknowledge, the Parties agree as follows.

I. Definitions

Capitalized terms not otherwise specifically defined herein shall have the meaning set forth in Appendix B, "Definitions." If the term is not defined herein or in the attached Appendix B, the definition in 45 CFR 155.20 shall apply.

II. Acceptance of Standard Rules of Conduct

ABE hereby acknowledges and agrees to accept and abide by the standard rules of conduct set forth below and in Appendix A, "Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities," while engaging in any activity as an Agent or Broker for purposes of facilitating enrollment through the FFEs or SBE-FPs. ABE shall be bound to and strictly adhere to the privacy and security standards, and to ensure that its Workforce that creates, collects, accesses, stores, maintains, discloses, or uses PII in the FFEs or SBE-FPs strictly adheres to the same.

a. Authorized Functions. ABE may create, collect, disclose, access, maintain, store, and use PII only for:

    1. Assisting with applications for QHP eligibility;

    2. Supporting QHP selection and enrollment by assisting with plan selection and plan comparisons;

    3. Assisting with applications for the receipt of APTC or CSRs, and selecting an APTC amount;

    4. Facilitating the collection of standardized attestations acknowledging the receipt of the APTC or CSRs determination, if applicable;

    5. Assisting with the application for and determination of certificates of exemption;

    6. Assisting with filing appeals of eligibility determinations in connection with the FFEs or SBE-FPs;

    7. Transmitting information about the Consumer's, Applicant's, Qualified Individual's, or Enrollee's decisions regarding QHP enrollment and/or CSRs and APTC information to the FFEs or SBE-FPs;

8. Facilitating payment of the initial premium amount for the appropriate QHP;
9. Facilitating an Enrollee's ability to disenroll from a QHP;
10. Educating Consumers, Applicants, Qualified Individuals, or Enrollees on Insurance Affordability Programs, and if applicable, informing such individuals of eligibility for Medicaid or Children's Health Insurance Program (CHIP);
11. Assisting an Enrollee's ability to report changes in eligibility status to an FFE or SBE-FP throughout the coverage year, including changes that may impact eligibility (e.g., adding a dependent);
12. Correcting errors in the application for QHP enrollment;
13. Informing or reminding Enrollees when QHP coverage should be renewed or when Enrollees may no longer be eligible to maintain their current QHP coverage because of age, or to inform Enrollees of QHP coverage options at renewal;
14. Providing appropriate information, materials, and programs to inform and educate Consumers, Applicants, Qualified Individuals, and Enrollees about the use and management of their health information and services and options offered through the selected QHP and among the available QHP options;
15. Contacting Consumers, Applicants, Qualified Individuals, and Enrollees to assess their satisfaction or resolve complaints with services provided by ABE in connection with the FFEs, SBE-FPs, or QHPs;
16. Providing assistance in communicating with QHP Issuers;
17. Carrying out ABE's legal responsibilities related to QHP Issuer functions in the FFEs or SBE-FPs, as permitted or required by ABE's contractual relationships with QHP Issuers; and
18. Other functions substantially similar to those enumerated above and such other functions that may be approved by CMS in writing from time to time.

An ABE may not under any circumstances create a HealthCare.Gov account for a consumer, log into a consumer's HealthCare.Gov account, log into HealthCare.Gov as a consumer, or create, collect, disclose, access, maintain, store, or use PII for such purposes.

b. PII Received. Subject to the terms and conditions of this Agreement and applicable laws, in performing the tasks contemplated under this Agreement, ABE may create, collect, disclose, access, maintain, store, and use the following data and PII from Consumers, Applicants, Qualified Individuals, and Enrollees, or these individuals' legal representative or Authorized Representative, including but not limited to:

- APTC percentage and amount applied
- Auto disenrollment information
- Applicant Name
- Applicant Address

- Applicant Birthdate
- Applicant Telephone number
- Applicant Email
- Applicant Social Security number
- Applicant spoken and written language preference
- Applicant Medicaid Eligibility indicator, start and end dates
- Applicant CHIP eligibility indicator, start and end dates
- Applicant QHP eligibility indicator, start and end dates
- Applicant APTC percentage and amount applied eligibility indicator, start and end dates
- Applicant household income
- Applicant Maximum APTC amount
- Applicant CSRs eligibility indicator, start and end dates
- Applicant CSRs level
- Applicant QHP eligibility status change
- Applicant APTC eligibility status change
- Applicant CSRs eligibility status change
- Applicant Initial or Annual Open Enrollment Indicator, start and end dates
- Applicant special enrollment period eligibility indicator and reason code
- Contact Name
- Contact Address
- Contact Birthdate
- Contact Telephone number
- Contact Email address
- Contact spoken and written language preference
- Enrollment group history (past six months)
- Enrollment type period
- FFE Applicant ID
- FFE Member ID
- Issuer Member ID
- Net premium amount
- Premium Amount, start and end dates
- Credit or Debit Card Number, Name on Card
- Checking account and routing number
- Special enrollment period reason
- Subscriber Indicator and relationship to subscriber
- Tobacco use indicator and last date of tobacco use
- Custodial parent
- Health coverage
- American Indian/Alaska Native status and name of tribe
- Marital status
- Race/ethnicity
- Requesting financial assistance
- Responsible person
- Applicant/Employee/dependent sex and name

- Student status
- Subscriber indicator and relationship to subscriber
- Total individual responsibility amount

c. Collection of PII. PII collected from Consumers, Applicants, Qualified Individuals, or Enrollees, or these individuals' legal representative or Authorized Representative, in the context of completing an application for QHP, APTC, or CSRs eligibility, or any data transmitted from or through the Hub, may be used only for the Authorized Functions specified in Section II.a of this Agreement. Such information may not be reused for any other purpose.

d. Collection and Use of Information Provided Under Other Authorities. This Agreement does not preclude ABE from separately collecting information from Consumers, Applicants, Qualified Individuals, or Enrollees, or their legal representative or Authorized Representative, for a non-FFE/non-SBE-FP/non-Hub purpose, and using, reusing, and disclosing such non-FFE/non-SBE-FP/non-Hub information obtained separately as permitted by applicable law and/or other applicable authorities. Such information must be separately collected and stored from any PII collected in accordance with Section II.c of this Agreement.

e. Ability of Consumer to Limit Collection and Use. ABE agrees to allow the Consumer, Applicant, Qualified Individual, or Enrollee, or these individuals' legal representative or Authorized Representative, to limit the ABE's creation, collection, use, maintenance, storage, and disclosure of their PII to the sole purpose of obtaining ABE's assistance in applying for QHP, APTC, or CSRs eligibility, and for performing the Authorized Functions specified in Section II.a of this Agreement.

III. Effective Date; Term and Renewal

a. Effective Date and Term. This Agreement becomes effective on the date that ABE electronically executes this Agreement and ends on the Day before the first day of the open enrollment period under 45 CFR 155.410(e)(2) for the benefit year beginning January 1, 2021.

b. Renewal. This Agreement may be renewed in the sole and absolute discretion of CMS for subsequent and consecutive one (1) year periods upon thirty (30) Days' advance written notice to ABE.

IV. **Termination**

a. Termination without Cause. Either Party may terminate this Agreement without cause and for its convenience upon thirty (30) Days' prior written notice to the other Party. Consistent with 45 CFR 155.220(f), ABE must include the intended date of termination in its notice. If a date is not specified, or the date is not acceptable to CMS, CMS may set a different termination date that is no less than 30 days from the date on the ABE's notice of termination. This Agreement shall automatically terminate at the end of its term (unless renewed as provided for in Section III.b of this Agreement) or in connection with the rejection of an amendment as provided for in Section VI.i of this Agreement.

b. Termination for Cause. The termination of this Agreement for cause and the reconsideration of any such termination shall be governed by the termination and reconsideration standards adopted by the FFEs under 45 CFR 155.220(g). Notwithstanding the foregoing, ABE shall be considered in "Habitual Default" of this Agreement in the event that it has been served with a non-compliance notice under 45 CFR 155.220(g) more than three (3) times in any calendar year, whereupon CMS may, in its sole discretion, immediately thereafter terminate this Agreement upon notice to ABE without any further opportunity to resolve the breach and/or non-compliance.

c. Termination for Failure to Maintain Valid State Licensure. ABE acknowledges and agrees that valid state licensure in each state in which ABE assists Consumers, Applicants, Qualified Individuals, or Enrollees in applying for or obtaining coverage under a QHP through an FFE or SBE-FP is a condition to ABE's authority under this Agreement. Accordingly, CMS may terminate this Agreement upon thirty (30) Days' prior written notice if ABE fails to maintain valid licensure in at least one FFE or SBE-FP state and in each state that ABE facilitates enrollment in a QHP through an FFE or SBE-FP. Any such termination shall be governed by the termination and reconsideration standards adopted by the FFEs under 45 CFR 155.220(g).

V. **Destruction of PII**

ABE covenants and agrees to destroy all PII in its possession at the end of the record retention period required under Appendix A. If, upon the termination or expiration of this Agreement, ABE has in its possession PII for which no retention period is specified in Appendix A, such PII shall be destroyed within 30 Days of the termination or expiration of this Agreement. ABE's duty to protect and maintain the privacy and security of PII, as provided for in Appendix A of this Agreement, shall continue in full force and effect until such PII is destroyed and shall survive the termination or expiration of this Agreement.

VI. **Miscellaneous**

a. Notice. All notices specifically required under this Agreement shall be given in writing and shall be delivered as follows:

If to CMS:

Centers for Medicare & Medicaid Services (CMS)
Center for Consumer Information & Insurance Oversight (CCIIO)
Attn: Office of the Director
Room 739H
200 Independence Avenue, SW
Washington, DC 20201

AgentBrokerCompliance@cms.hhs.gov

If to ABE, to ABE's address, including email address, on record in ABE's MLMS account.

Notices sent by hand, by overnight courier service or via email, or mailed by certified or registered mail, shall be deemed to have been given when received; notices sent by facsimile shall be deemed to have been given when the appropriate confirmation of receipt has been received; notices not given on a business day (i.e., Monday – Friday excluding Federal holidays) between 9:00 a.m. and 5:00 p.m. local time where the recipient is located shall be deemed to have been given at 9:00 a.m. on the next business day for the recipient. Either Party to this Agreement may change its contact information for notices and other communications by providing 30 Days' written notice of such change in accordance with this provision.

b. Assignment and Subcontracting. ABE shall not assign this Agreement in whole or in part, whether by merger, acquisition, consolidation, reorganization, or otherwise, nor subcontract any portion of the services to be provided by ABE under this Agreement, nor otherwise delegate any of its obligations under this Agreement, without the express, prior written consent of CMS, which consent may be withheld, conditioned, granted, or denied in CMS's sole and absolute discretion. ABE further shall not assign this Agreement or any of its rights or obligations hereunder without the express, prior written consent of CMS. If ABE attempts to make an assignment, subcontract its service obligations or otherwise delegate its obligations hereunder in violation of this provision, such assignment, subcontract, or delegation shall be deemed void *ab initio* and of no force or effect, and ABE shall remain legally bound hereto and responsible for all obligations under this Agreement. ABE shall further be thereafter subject to such compliance actions as may otherwise be provided for under applicable law.

c. Survival. ABE's duty to protect and maintain the privacy and security of PII under this Agreement shall survive the expiration or earlier termination of this Agreement.

d. Severability. The invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement. In the event that any provision of this Agreement is determined to be invalid, unenforceable or otherwise illegal, such provision shall be deemed restated, in accordance with applicable law, to reflect as nearly as possible the original intention of the parties, and the remainder of the Agreement shall be in full force and effect.

e. Disclaimer of Joint Venture. Neither this Agreement nor the activities of ABE contemplated by and under this Agreement shall be deemed or construed to create in any way any partnership, joint venture, or agency relationship between the Parties. Neither Party is, nor shall either Party hold itself out to be, vested with any power or right to bind the other Party contractually or to act on behalf of the other Party, except to the extent expressly set forth in the PPACA and the regulations codified thereunder, including as codified at 45 CFR part 155.

f. Remedies Cumulative. No remedy herein conferred upon or reserved to CMS under this Agreement is intended to be exclusive of any other remedy or remedies available to CMS under operative law and regulation, and each and every such remedy, to the extent permitted by law, shall be cumulative and in addition to any other remedy now or hereafter existing at law or in equity or otherwise.

g. Compliance with Law. ABE covenants and agrees to comply with any and all applicable laws, statutes, regulations, or ordinances of the United States of America, and any Federal Government agency, board or court, that are applicable to the conduct of the activities that are the subject of this Agreement, including but not necessarily limited to, any additional and applicable standards required by statute, and any regulations or policies implementing or interpreting such statutory provisions hereafter issued by CMS. In the event of a conflict between the terms of this Agreement and any statutory, regulatory, or sub-regulatory guidance released by CMS, the requirement that constitutes the stricter, higher, or more stringent level of compliance shall control.

h. Governing Law and Consent to Jurisdiction. This Agreement will be governed by the laws and common law of the United States of America, including without limitation such regulations as may be promulgated from time to time by HHS or any of its constituent agencies, without regard to any conflict of laws statutes or rules. ABE further agrees and consents to the jurisdiction of the Federal Courts located within the District of Columbia and the courts of appeal therefrom, and waives any claim of lack of jurisdiction or *forum non conveniens*.

i. Amendment. CMS may amend this Agreement for purposes of reflecting changes in applicable law or regulations, with such amendments taking effect upon thirty (30)-Days' written notice to ABE ("CMS notice period"). Any amendments made under this provision will only have prospective effect and will not be applied retrospectively. ABE may reject such amendment, by providing to CMS, during the CMS notice period, thirty (30)-Days' written notice of its intent to reject the amendment ("rejection notice period"). Any such rejection of an amendment made by CMS shall result in the termination of this Agreement upon expiration of the rejection notice period.

j. Audit. ABE agrees that CMS, the Comptroller General, the Office of the Inspector General of HHS, or their designees have the right to audit, inspect, evaluate, examine, and make excerpts, transcripts, and copies of any books, records, documents, and other evidence of ABE compliance with the requirements of this Agreement, upon reasonable notice to ABE and during ABE's regular business hours and at ABE's regular business location. ABE further agrees to allow reasonable access to the information and facilities requested by CMS, the Comptroller General, the Office of the Inspector General of HHS, or their designees for the purpose of such an audit.

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 Patient Protection and Affordable Care Act (42 U.S.C. § 18081(g)) and 45 CFR 155.260. Capitalized terms not otherwise specifically defined herein shall have the meaning assigned in Appendix B, "Definitions." If the term is not defined herein or in Appendix B, the definition in 45 CFR 155.20 shall apply.

The standards and implementation specifications that are set forth in this Appendix A are consistent with the principles in 45 CFR 155.260(a)(1) through (a)(6), including being at least as protective as the privacy and security standards and implementation specifications that we have established for the Federally-Facilitated Exchanges ("FFEs").

The FFEs will enter into contractual agreements with all Non-Exchange Entities that gain access to Personally Identifiable Information ("PII") exchanged with the FFEs or SBE-FPs, or directly from Consumers, Applicants, Qualified Individuals, and Enrollees, or these individuals' legal representatives or Authorized Representatives. That agreement and its appendices, including this Appendix A, govern any PII that is created, collected, disclosed, accessed, maintained, stored, or used by Non-Exchange Entities in the context of an FFE or SBE-FP. In signing that contractual agreement, in which this Appendix A has been incorporated, Non-Exchange Entities agree to comply with the standards and implementation specifications laid out in this document and the applicable standards, controls, and applicable implementation specifications within the privacy and security standards as established by the FFEs under 45 CFR 155.260(a)(3) and as applicable to non-Exchange entities under 45 CFR 155.260(b)(3) while performing the Authorized Functions outlined in their respective agreements.

NON-EXCHANGE ENTITY PRIVACY AND SECURITY STANDARDS AND IMPLEMENTATION SPECIFICATIONS

Non-Exchange Entities must meet the following privacy and security standards.

(1) Individual Access to PII: In keeping with the standards and implementation specifications used by the FFEs, Non-Exchange Entities that maintain and/or store PII must provide Consumers, Applicants, Qualified Individuals, and Enrollees, or these individuals' legal representatives and Authorized Representatives, 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 CMS.

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 Consumers, Applicants, Qualified Individuals, and Enrollees 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, and Enrollee—or these individuals' legal representatives or Authorized Representatives—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. The Non-Exchange Entity may charge a fee only to recoup the 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 recipient 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.

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. 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 FFEs, Non-Exchange Entities must ensure openness and transparency about policies, procedures, and technologies that directly affect Consumers, Applicants, Qualified Individuals, and Enrollees 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 it 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 FFEs, Non-Exchange Entities should ensure that Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—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, and Enrollees—or these individuals' legal representatives or Authorized Representatives—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 an FFE, SBE-FP, 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 FFEs, 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, or Enrollee.

a. Standard: Creation, Collection, Disclosure, Access, Maintenance, Storage, and Use Limitations. 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:

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

   ii. 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 in Section (3) above; and/or

   iii. 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, or Enrollee, 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 QHPs.

(5) Data Quality and Integrity. In keeping with the standards and implementation specifications used by the FFEs, 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 FFEs, Non-Exchange Entities must offer Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—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 ten (10) business days of receipt.

4. If the Non-Exchange Entity (or its 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 Non-Exchange Entity (or its 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 FFEs, 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 modification—including 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 modification—including amendment, correction, substitution, or deletion—of a Consumer's, Applicant's, Qualified Individual's, or Enrollee'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, all 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 ten (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, and Enrollees—or these individuals' legal representatives or Authorized Representatives—on their request per the procedures outlined under the access standards in Section (1) above.

(6) Accountability. Non-Exchange Entities must adopt and implement the privacy and security standards and implementation specifications described in this document that have been established by the FFEs under 45 CFR 155.260(b) 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 one hour of discovery.

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

[1] Available at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-8-Incident-Response.pdf

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 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.

c. 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 FFEs is sufficient to satisfy the requirements of this paragraph.

(7) Safeguarding PII. In keeping with the standards and implementation specifications used by the FFEs, a Non-Exchange Entity must ensure that PII is protected with reasonable operational, administrative, technical, and physical safeguards to ensure its

confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.

a. Standard: Security Controls. The Non-Exchange Entity is required to establish and implement operational, technical, administrative, and physical safeguards that are consistent with any applicable laws and ensure that:

   i. PII is only used by or disclosed to those authorized to receive or view it;

   ii. PII is protected against any reasonably anticipated threats or hazards to the confidentiality, integrity, and availability of such information;

   iii. PII is protected against any reasonably anticipated uses or disclosures of such information that are not permitted or required by law; and

   iv. PII is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with retention schedules.

b. Standard: Required Monitoring of Security Controls. A Non-Exchange Entity must monitor, periodically assess, and update its security controls and related system risks to ensure the continued effectiveness of those controls.

c. Standard: A Non-Exchange Entity must develop and utilize secure electronic interfaces when transmitting PII electronically.

APPENDIX B
DEFINITIONS

This Appendix defines terms that are used in the Agreement and other Appendices. Any capitalized term used in the Agreement or Appendix A that are not defined therein and are also not defined here in Appendix B has the meaning provided in 45 CFR 155.20.

(1) **Access** means availability of a System of Records Notice (SORN) Record to a subject individual.

(2) **Advance Payments of the Premium Tax Credit (APTC)** has the meaning set forth in 45 CFR 155.20.

(3) **Agent** or **Broker** has the meaning set forth in 45 CFR 155.20.

(4) **Applicant** has the meaning set forth in 45 CFR 155.20.

(5) **Application Filer** has the meaning set forth in 45 CFR 155.20.

(6) **Authorized Function** means a task performed by a Non-Exchange Entity that the Non-Exchange Entity is explicitly authorized or required to perform based on applicable law or regulation, and as enumerated in the Agreement that incorporates this Appendix B.

(7) **Authorized Representative** means a person or organization meeting the requirements set forth in 45 CFR 155.227.

(8) **Breach** is defined in the Glossary of Office of Management and Budget (OMB) Memorandum M-17-12 (January 3, 2017) and means 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 personally identifiable information for an other than authorized purpose.

(9) **CCIIO** means the Center for Consumer Information and Insurance Oversight within the Centers for Medicare & Medicaid Services (CMS).

(10) **CMS** means the Centers for Medicare & Medicaid Services.

(11) **CMS Companion Guides** means a CMS-authored guide, available on the CMS web site, which is meant to be used in conjunction with and supplement relevant implementation guides published by the Accredited Standards Committee.

(12) **CMS Data Services Hub (Hub)** is the CMS Federally-managed service to interface data among connecting entities, including HHS, certain other Federal agencies, and State Medicaid agencies.

(13) **CMS Data Services Hub Web Services (Hub Web Services)** means business and technical services made available by CMS to enable the determination of certain eligibility and enrollment or Federal financial payment data through the FFE or SBE-FP website, including the collection of personal and financial information

necessary for Consumer, Applicant, Qualified Individual, Qualified Employer, Qualified Employee, or Enrollee account creations; QHP application submissions; and Insurance Affordability Program eligibility determinations.

(14) **Compliance and Oversight Activities** are the routine activities and processes conducted by a QHP Issuer, Agent, Broker, or Web-broker as related to ensuring operational integrity, including but not limited to internal reviews and audits of business procedures and processes and maintaining records as required by State or Federal law.

(15) **Consumer** means a person who, for himself or herself, or on behalf of another individual, seeks information related to eligibility or coverage through a QHP or other Insurance Affordability Program, or whom an Agent or Broker (including Web-brokers), Navigator, Issuer, Certified Application Counselor, or other entity assists in applying for a coverage through QHP, applying for APTC and CSRs, and/or completing enrollment in a QHP through the Individual Market FFEs or SBE-FPs.

(16) **Controlling Health Plan (CHP)** has the meaning set forth in 45 CFR 162.103.

(17) **Cost-sharing Reductions (CSRs)** has the meaning set forth in 45 CFR 155.20.

(18) **Customer Service** means assistance regarding Health Insurance Coverage provided to a Consumer, Applicant, Qualified Individual, Qualified Employer, or Qualified Employee, including but not limited to responding to questions and complaints and providing information about Health Insurance Coverage and enrollment processes in connection with an FFE or SBE-FP.

(19) **Day or Days** means calendar days unless otherwise expressly indicated in the relevant provision of the Agreement that incorporates this Appendix B.

(20) **Department of Insurance (DOI)** means the State agency or regulatory authority that, among other things, licenses, oversees, and regulates Issuers, Agents, and Brokers, as applicable.

(21) **Designated Privacy Official** means a contact person or office responsible for receiving complaints related to Breaches or Incidents, able to provide further information about matters covered by the notice, responsible for the development and implementation of the privacy and security policies and procedures of the Non-Exchange Entity, and ensuring the Non-Exchange Entity has in place appropriate safeguards to protect the privacy and security of PII.

(22) **Enrollee** has the meaning set forth in 45 CFR 155.20.

(23) **Enrollment Reconciliation** is the process set forth in 45 CFR 155.400(d).

(24) **Exchange** has the meaning set forth in 45 CFR 155.20.

(25) **Federally-facilitated Exchange (FFE)** means an **Exchange** (or **Marketplace**) established by HHS and operated by CMS under Section 1321(c)(1) of the Patient

Protection and Affordable Care Act for individual or small group market coverage, including the Federally-facilitated Small Business Health Options Program (**FF-SHOP**). **Federally-facilitated Marketplace (FFM)** has the same meaning as FFE.

(26) **Federal Privacy Impact Assessment (PIA)** is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks, as defined in OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 26, 2003).

(27) **Health Insurance Coverage** has the meaning set forth in 45 CFR 155.20.

(28) **Health Insurance Exchanges Program (HIX)** means the System of Records that CMS uses in the administration of the FFEs and SBE-FPs. As a System of Records, the use and disclosure of the SORN Records maintained by the HIX must comply with the Privacy Act of 1974, the implementing regulations at 45 CFR Part 5b, and the "routine uses" that were established for the HIX in the Federal Register at 78 Fed.Reg. 8538 (February 6, 2013), as amended by 78 Fed.Reg. 32256 (May 29, 2013) and 78 Fed.Reg. 63211 (October 23, 2013).

(29) **HHS** means the U.S. Department of Health & Human Services.

(30) **Health Insurance Portability and Accountability Act (HIPAA)** means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, as amended, and its implementing regulations.

(31) **Incident**, or **Security Incident** is defined in the Glossary of Office of Management and Budget (OMB) Memorandum M-17-12 (January 3, 2017) and 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.

(32) **Information** means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

(33) **Insurance Affordability Program** means a program that is one of the following:

(1) A State Medicaid program under title XIX of the Social Security Act.

(2) A State children's health insurance program (CHIP) under title XXI of the Social Security Act.

(3) A State basic health program established under section 1331 of the Patient Protection and Affordable Care Act.

(4) A program that makes coverage in a Qualified Health Plan through the Exchange with Advance Payments of the Premium Tax Credit established under section 36B of the Internal Revenue Code.

(5) A program that makes available coverage in a Qualified Health Plan through the Exchange with Cost-sharing Reductions established under section 1402 of the Patient Protection and Affordable Care Act.

(34) **Issuer** has the meaning set forth in 45 CFR 144.103.

(35) **Non-Exchange Entity** has the meaning at 45 CFR 155.260(b), including but not limited to Navigators, Agents, Brokers, and Web-brokers.

(36) **OMB** means the Office of Management and Budget.

(37) **Other Entity Identifier (OEID)** means an identifier that an entity uses to identify itself or have itself identified on all covered transactions in which it needs to be identified or for any other lawful purpose and is available through the Enumeration System identified in 45 CFR 162.508 to an entity that:

(1) Needs to be identified in a transaction for which the Secretary of HHS has adopted a standard under 45 CFR Part 162;

(2) Is not eligible to obtain a Health Plan Identifier under 45 CFR 162.506;

(3) Is not eligible to obtain a National Provider Identifier (NPI) under 45 CFR 160.410; and

(4) Is not an individual.

(38) **Patient Protection and Affordable Care Act (PPACA)** means the Patient Protection and Affordable Care Act (Public Law 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law 111-152), which are referred to collectively as the Patient Protection and Affordable Care Act.

(39) **Personally Identifiable Information (PII)** has the meaning contained in the Glossary of Office of Management and Budget (OMB) Memorandum M-17-12 (January 3, 2017) and means 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.

(40) **Qualified Employee** has the meaning set forth in 45 CFR 155.20.

(41) **Qualified Employer** has the meaning set forth in 45 CFR 155.20.

(42) **Qualified Health Plan (QHP)** has the meaning set forth in 45 CFR 155.20.

(43) **Qualified Individual** has the meaning set forth in 45 CFR 155.20.

(44) **Responsible Official** means an individual or officer responsible for managing a Non-Exchange Entity or Exchange's records or information systems, or another individual designated as an individual to whom requests can be made, or the

designee of either such officer or individual who is listed in a Federal System of Records Notice as the system manager, or another individual listed as an individual to whom requests may be made, or the designee of either such officer or individual.

(45) **Security Control** means a safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

(46) **State** means a State that has licensed the Agent, Broker, or Web-broker that is a party to this Agreement and in which the Agent, Broker, or Web-broker is operating.

(47) **State-based Exchange on the Federal Platform (SBE-FP)** means an **Exchange** (or **Marketplace**) established by a State that receives approval under 45 CFR 155.106(c) to utilize the Federal platform to support select eligibility and enrollment functions, including for the Small Business Health Options Program (**SBE-FP SHOP**). **State-based Marketplace on the Federal Platform (SBM-FP)** has the same meaning as SBE-FP.

(48) **State Partnership Exchange** means a type of FFE in which a State assumes responsibility for carrying out certain activities related to plan management, consumer assistance, or both.

(49) **Subhealth Plan (SHP)** has the meaning set forth in 45 CFR 162.103.

(50) **Subject Individual** means that individual to whom a SORN Record pertains.

(51) **System of Records** means a group of Records under the control of any Federal agency from which information is retrieved by name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

(52) **System of Records Notice (SORN)** means a notice published in the Federal Register notifying the public of a System of Records maintained by a Federal agency. The notice describes privacy considerations that have been addressed in implementing the system.

(53) **System of Record Notice (SORN) Record** means any item, collection, or grouping of information about an individual that is maintained by an agency, including but not limited to that individual's education, financial transactions, medical history, and criminal or employment history and that contains that individual's name, or an identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph, that is part of a System of Records.

(54) **Trading Partner** means an entity that exchanges enrollment or financial management data with a Hub contractor.

(55) **Web-broker** means an individual Agent or Broker, or group of Agents or Brokers, or business entity registered with an Exchange under §155.220(d)(1) that develops and hosts a non-Exchange website that interfaces with an Exchange to assist consumers with direct enrollment in qualified health plans offered through the Exchange as described in 45 CFR 155.220(c)(3) and 155.221. The term also includes a direct enrollment technology provider.

(56) **Workforce** means a Non-Exchange Entity's, FFE's, SBE-FP's employees, agents, contractors, subcontractors, officers, directors, agents, representatives, and any other individual who may create, collect, disclose, access, maintain, store, or use PII in the performance of his or her duties.