UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

FORM 8-K

CURRENT REPORT
PURSUANT TO SECTION 13 OR 15(d)
OF THE SECURITIES EXCHANGE ACT OF 1934

Date of Report (date of earliest event reported): October 30, 2016

EHEALTH, INC.

(Exact Name of Registrant as Specified in its Charter)

Delaware	**001-33071**	**56-2357876**
(State or other jurisdiction of incorporation)	(Commission File Number)	(I.R.S. Employer Identification No.)

440 EAST MIDDLEFIELD ROAD
MOUNTAIN VIEW, CALIFORNIA 94043
(Address of principal executive offices) (Zip Code)

(650) 584-2700
(Registrant's telephone number, including area code)

Not Applicable
(Former name or former address, if changed since last report)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions:

o Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)

o Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)

o Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))

o Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Item 7.01. Regulation FD Disclosure.

Agreements with the Centers for Medicare & Medicaid Services

On October 30, 2016, eHealth, Inc. (the "Company") (through its subsidiary eHealthInsurance Services, Inc.) entered into an "Agreement Between Web-Based Entity and the Centers for Medicare and Medicaid Services for the Federally-Facilitated Exchange and the State-Based Exchange on the Federal Platform Individual Market" (the "CMS Agreement"). The CMS Agreement replaces the terms of a previous agreement that the Company entered into with the Centers for Medicare and Medicaid Services (the "CMS") which expired on October 31, 2016. CMS is the government agency that is responsible for the management and oversight of the Federally-facilitated marketplace ("FFM") created under the Patient Protection and Affordable Care Act of 2010, as amended (the "Affordable Care Act").

Under the Affordable Care Act, each state in the United States is required to create a government-run health insurance exchange through which individuals may among other things (i) enroll in health insurance coverage under a qualified health plan ("QHP"); and (ii) apply for advance payments of premium tax credits and cost-sharing reductions for QHPs (hereinafter, "subsidies"). In order for an individual to receive a subsidy, the individual must enroll in a QHP through the government-run exchange. In the event a state determines not to establish a health insurance exchange, CMS is permitted to operate the FFM as the health insurance exchange for that state. Under the Affordable Care Act, a state may permit health insurance agents such as the Company to enroll individuals into QHPs through the health insurance exchange.

Pursuant to regulations issued by the Department of Health and Human Services, an agent or broker that desires to enroll individuals into qualified health plans through a government-run health insurance exchange, including the FFM, must meet several conditions and requirements, including additional conditions and requirements if the website of the agent or broker is used to complete QHP selection. The Company's entering into the CMS Agreement is one of those conditions and requirements. Provided that the Company satisfies the terms and conditions of the CMS Agreement, the CMS Agreement permits the Company to (i) receive certain personally identifiable information held in the health insurance exchange program; (ii) gain access to business and technical services provided by CMS that would enable the Company to establish a connection to the FFM; and (iii) create, collect, disclose, access, maintain, store and use personally identifiable information from CMS and individuals who are eligible for, enrolled in or seeking information regarding QHPs. The CMS Agreement defines the set of information that the Company may create, collect, disclose, access, maintain, store and use and places restrictions on the Company's use and disclosure of such information. Moreover, the agreement contains privacy and security standards and implementation specifications that the Company must meet in order to have access, and continue to have access, to the information necessary to enroll individuals into QHPs through the FFM and to assist individuals in applying for subsidies. The term of the CMS Agreement ends on the day before the first day of the open enrollment period for the benefit year beginning January 1, 2018, after which the agreement may be renewed for subsequent and consecutive one (1) year periods subject to CMS' sole and absolute discretion. In addition, the CMS Agreement may be terminated for convenience upon thirty (30) day's prior written notice by either the Company or CMS and may be terminated for cause in accordance with termination standards adopted under applicable regulations. Moreover, CMS may amend the CMS Agreement upon 30-day's notice to reflect changes in applicable law or regulations. All agents and brokers who use their internet website to assist individuals in applying for qualified health plans and subsidies through the FFM ("WBEs") are required to enter into the CMS Agreement.

Robert Hurley, an executive officer at the Company and a primary writing agent for the Company, as well as certain other individually licensed health insurance agents, also entered into two agreements (the "CMS Agent Agreements") with CMS in the form attached hereto as Exhibit 99.2. All agents and brokers, including those that do not use their internet website to assist individuals in applying for qualified health plans and subsidies through the FFM, are required to enter into the CMS Agent Agreements. The CMS Agent Agreements contain requirements that must be met in order to enroll eligible individuals in qualified health plans through the FFM. The CMS Agent Agreements provide that in order to do so the agent must (i) register with the FFM; (ii) receive training in the range of QHP options and insurance affordability programs offered through the FFM; (iii) comply with comprehensive privacy and security standards adopted by the FFM; (iv) comply with all other applicable laws, statutes, regulations,

ordinances and guidance issued or to be issued; and (v) maintain valid licensure in each state where the agent offers QHPs through the FFM. The terms of the CMS Agent Agreements end on the day before the first day of the open enrollment period for the benefit year beginning January 1, 2018, after which the agreements may be renewed for subsequent and consecutive one (1) year periods subject to CMS' sole and absolute discretion. CMS may also amend the agreements to incorporate any additional standards required by statute, regulation or policy implementing or interpreting such statutory or regulatory provisions. Moreover, statutory, regulatory and sub-regulatory guidance released by CMS controls over the terms of the CMS Agent Agreements.

While the Company has entered into the CMS Agreement and individuals at the Company have entered into the CMS Agent Agreements, there are risks and uncertainties relating to the Company's ability to enroll individuals into qualified health plans through the FFM and to assist those individuals in applying for subsidies. Among other things, the Company must satisfy the requirements contained in the CMS Agreement, the CMS Agent Agreements and applicable laws, regulations and regulatory guidance; maintain a compliant web platform incorporating those requirements; obtain qualified health plan information from the Company's health insurance carrier partners and CMS and incorporate it into its web platform; maintain a privacy and security program to conform to the privacy and security requirements of the CMS Agreement and CMS Agent Agreements as well as laws, regulations and regulatory guidance applicable to the Company acting as a WBE; and successfully adopt and maintain solutions to integrate with FFM systems so that information may be passed to and from the Company and the FFM relating to enrollment in qualified health plan and subsidy eligibility. In addition, the Company is dependent upon the operability of the FFM website and systems to be able to enroll individuals in QHPs through the FFM, and any change to, failure of or interruption in the availability of the website or systems could harm the ability of the Company to enroll individuals into QHPs. The Company depends upon the FFM for a number of other things relating to the Company's ability to enroll individuals into qualified health plans, including integration with the FFM as well as certain qualified health plan information required under the applicable regulations to be displayed on the Company's website. Moreover, individual states participating in the FFM may determine not to allow agents and brokers such as the Company to enroll individuals in QHPs through the FFM. In addition, CMS directed the Company to alter the online process it developed for enrolling subsidy-eligible individuals in QHPs through the FFM. As a result of the changes that the Company made to its online process after the last open enrollment period in response to CMS requirements, the Company experienced a substantial reduction in the rate at which individuals and families starting the application process for QHPs and subsidies became members. To date, CMS has not made meaningful improvements to the process and has declined the Company's request to make changes. The Company expects that the reduced conversion rates for the process that CMS has directed the Company to use for enrolling individuals in QHPs will persist during the open enrollment period that began on November 1, 2016 and is scheduled to end January 31, 2017.

The foregoing description of the terms of the CMS Agreement and the CMS Agent Agreements does not purport to be complete. The CMS Agreement and the CMS Agent Agreements are qualified in their entirety by reference to the full text of the CMS Agreement and the CMS Agent Agreements, copies of which are attached hereto as Exhibits 99.1 and 99.2. In addition, the discussion of aspects of the Affordable Care Act and related regulations are merely summaries of aspects of complex laws and do not purport to be complete summaries.

This Current Report on Form 8-K contains forward-looking statements, including statements regarding the Affordable Care Act and the related regulations, the FFM's expected operation of health insurance exchanges during the open enrollment period that began on November 1, 2016, the obligation of eligible individuals to purchase qualified health plans through a government-run health insurance exchange, the Company's ability to enroll individuals in qualified health plans through the FFM and expected reduction in conversion rates. These forward-looking statements involve certain risks and uncertainties that could cause actual results to differ materially from those indicated in such forward-looking statements, including, but not limited to, the Company's ability to enroll individuals in qualified health plans through the FFM; the Company's ability to maintain our agreements with the CMS which need to be renewed every year; the Company's ability to satisfy the conditions and requirements contained in the CMS Agreement and the CMS Agent Agreements, applicable laws, regulations and regulatory guidance; the Company's ability to maintain a compliant web platform incorporating the requirements of the CMS Agreement, the CMS Agent Agreements, and applicable laws, regulations and regulatory guidance; the Company's ability to obtain qualified health plan information from the Company's health insurance carrier partners and CMS

and incorporate it into its web platform; the Company's ability to maintain a privacy and security program to conform to the privacy and security requirements of the CMS Agreement and CMS Agent Agreements as well as laws, regulations and regulatory guidance applicable to the Company acting as a WBE; the Company's ability to adopt and maintain solutions to integrate with the FFM so that information may be passed to and from the Company relating to enrollment in qualified health plan and subsidy eligibility; the availability and reliability of the FFM website and systems; and the Company's ability to timely meet the applicable requirements and potential changes in laws, regulations and regulatory guidance. Other risks and uncertainties that can affect actual results are included under the captions "Risk Factors" and "Management's Discussion and Analysis of Financial Condition and Results of Operations" in our Annual Report on Form 10-K for the year ended December 31, 2015 and our most recent Quarterly Report on Form 10-Q, which are on file with the SEC and are available on the investor relations page of the Company's website at *http://www.ehealthinsurance.com* and on the Securities and Exchange Commission's website at *www.sec.gov* . All information provided in this Current Report on Form 8-K is as of the date of its filing, and we undertake no duty to update this information unless required by law. The information in Item 7.01 of this Current Report on Form 8-K and the exhibits attached hereto shall be deemed "furnished" and shall not be deemed "filed" for purposes of Section 18 of the Securities Exchange Act of 1934, as amended. Except as shall be expressly set forth by specific reference in such filing, the information contained herein and in the accompanying exhibits shall not be incorporated by reference into any filing with the Securities and Exchange Commission made by the company, whether made before or after the date hereof, regardless of any general incorporation language in such filing.

Item 9.01. Financial Statements and Exhibits

(d) Exhibits.

Exhibit Number	Description
99.1	Agreement between Web-Based Entity and the Centers for Medicare & Medicaid Services for the Federally-Facilitated Exchange and the State-Based Exchange on the Federal Platform Individual Market between eHealthInsurance Services, Inc. and the Centers for Medicare & Medicaid Services.
99.2	Form of Agreements between Agent or Broker and the Centers for Medicare & Medicaid Services for Individual Market Federally-Facilitated Exchanges and State-Based Exchanges on the Federal Platform.

SIGNATURE

Pursuant to the requirements of the Securities Exchange Act of 1934, as amended, the registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

Date: November 3, 2016

/s/ Scott Giesler

Scott Giesler

Senior Vice President, General Counsel & Secretary

EXHIBIT INDEX

Exhibit Number	Description
99.1	Agreement between Web-Based Entity and the Centers for Medicare & Medicaid Services for the Federally-Facilitated Exchange and the State-Based Exchange on the Federal Platform Individual Market between eHealthInsurance Services, Inc. and the Centers for Medicare & Medicaid Services.
99.2	Form of Agreements between Agent or Broker and the Centers for Medicare & Medicaid Services for Individual Market Federally-Facilitated Exchanges and State-Based Exchanges on the Federal Platform.

AGREEMENT BETWEEN WEB-BASED ENTITY AND THE CENTERS FOR MEDICARE & MEDICAID SERVICES FOR THE FEDERALLY-FACILITATED EXCHANGE AND THE STATE-BASED EXCHANGE ON THE FEDERAL PLATFORM INDIVIDUAL MARKET

THIS WEB-BROKER 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 operation of the Federal eligibility and enrollment platform relied upon by certain State-based Exchanges for their eligibility and enrollment functions (SBE-FPs), including the CMS Data Services Hub ("Hub"), and eHealthInsurance Services, Inc., (hereinafter referred to as Web-based Entity or "WBE"), an Agent or Broker that uses a non-FFE Internet website in accordance with 45 CFR 155.220(c)(3) to assist Consumers, Applicants, Qualified Individuals, and Enrollees in applying for Advance Payments of the Premium Tax Credits ("APTCs") and Cost-sharing Reductions ("CSRs") for Qualified Health Plans ("QHPs"), and/or in completing enrollment in QHPs offered in the individual market through the FFEs or SBE-FPs, and provides Customer Service (CMS and WBE hereinafter referred to as the "Party," or collectively, as the "Parties").

WHEREAS:

1. Section 1312(e) of the Affordable Care Act ("ACA") 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 APTCs and CSRs, to the extent allowed by States. To participate in an FFE or SBE-FP, Agents and Brokers, including WBEs, must complete all necessary registration and training requirements under 45 CFR 155.220.

2. To facilitate the eligibility determination and enrollment processes, CMS will provide centralized and standardized business and technical services ("Hub Web Services") through an application programming interface to WBE that will enable WBE to establish a secure connection with the Hub. The application programming interface will enable the secure transmission of key eligibility and enrollment information between CMS and WBE.

3. To facilitate the operation of the FFEs and SBE-FPs, CMS desires to: (a) disclose Personally Identifiable Information ("PII"), which is held in the Health Insurance Exchanges Program ("HIX"), to WBE; (b) provide WBE with access to the Hub Web Services; and (c) permit WBE to create, collect, disclose, access, maintain, store, and use PII from CMS, Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—to the extent that these activities are necessary to carry out the functions that the ACA and implementing regulations permit WBE to carry out.

4. WBE is an entity licensed as an Agent or Broker and desires to gain access to the

Hub Web Services, and 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.

5. 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 156.260(a)(1) through (a)(6), including being at least as protective as the standards the Exchange has established and implemented for itself under 45 CFR 155.260(a)(3), as a condition of contract or agreement with Non-Exchange Entities, and WBE is a Non-Exchange Entity.

6. CMS, in the administration of the FFEs and the Hub, 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 the attached Appendix B, "Definitions." Any capitalized term that is not defined herein or in Appendix B has the meaning provided in 45 CFR 155.20.

II. Acceptance of Standard Rules of Conduct.

WBE and CMS are entering into this Agreement to satisfy the requirements under 45 CFR 155.260(b)(2). WBE 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," and Appendix C, "Standards for Communication with the Hub," which are incorporated by reference in this Agreement, while and as engaging in any activity as WBE for purposes of the ACA. WBE shall be bound to strictly adhere to the privacy and security standards—and to ensure that its employees, officers, directors, contractors, subcontractors, agents, and representatives strictly adhere to the same—to gain and maintain access to the Hub Web Services and to create, collect, disclose, access, maintain, store, and use PII for the efficient operation of the FFEs and SBE-FPs.

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

    1. Assisting with completing applications for QHP eligibility;
    2. Supporting QHP selection and enrollment by assisting with plan selection and plan comparisons;
    3. Assisting with completing applications for the receipt of APTCs or CSRs and with selecting an APTC amount;

4. Facilitating the collection of standardized attestations acknowledging the receipt of the APTC or CSR 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 and SBE-FPs;
7. Transmitting information about the Consumer's, Applicant's, Qualified Individual's, or Enrollee's decisions regarding QHP enrollment and/or CSR and APTC information to the FFEs and SBE-FPs;
8. Facilitating payment of the initial premium amount to the appropriate QHP;
9. Facilitating an Enrollee's ability to disenroll from a QHP;
10. Educating Consumers, Applicants, 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 the FFEs and SBE-FPs throughout the coverage year, including changes that may affect 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, 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 Consumers, Applicants, Qualified Individuals, and Enrollees, to inform and educate them about the use and management of their health information, and services and options offered through the selected QHP or among the available QHP options;
15. Contacting Consumers, Applicants, Qualified Individuals, and Enrollees to assess their satisfaction or resolve complaints with services provided by WBE in connection with the FFEs, SBE-FPs, WBE, or QHPs;
16. Providing assistance in communicating with QHP Issuers;
17. Fulfilling the legal responsibilities related to the efficient functions of QHP Issuers in the FFEs and SBE-FPs, as permitted or required by WBE's contractual relationships with QHP Issuers; and
18. Performing other functions substantially similar to those enumerated above and such other functions that CMS may approve in writing from time to time.

b. Standards Regarding PII.
WBE agrees that it will create, collect, disclose, access, maintain, use, or store PII that it receives directly from Consumers, Applicants, Qualified Individuals, or Enrollees and from Hub Web Services only in accordance with all laws as applicable, including section 1411(g) of the ACA.

1. Safeguards. WBE agrees to monitor, periodically assess, and update its security controls and related system risks to ensure the continued effectiveness of those controls in accordance with this Agreement, including Appendix A, "Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities," and to timely inform the Exchange of any material change in its administrative, technical, or operational environments, or that would require an alteration of the privacy and security standards within this Agreement.
2. Downstream Entities. WBE will satisfy the requirement in 45 CFR 155.260(b)(2)(v) to bind downstream entities by entering into written agreements with any downstream entities that will have access to PII as defined in this Agreement.
3. Critical Security and Privacy Controls. The critical controls the WBE must implement before WBE is able to submit any transactions to the FFE production system:
    a. Email/Web Browser Protections – Including but not limited to assurance that transfer protocols are secure and limits the threat of communications being intercepted.
    b. Malware Protection – Including but not limited to protections against known threat vectors within the system's environment to mitigate damage/security breaches.
    c. Patch Management – Including but not limited to ensuring every client and server is up to date with the latest security patches throughout the environment.
    d. Vulnerability Management – Including but not limited to identifying, classifying, remediating, and mitigating vulnerabilities on a continual basis by conducting periodic vulnerability scans to identify weaknesses within an environment.
    e. Inventory of Software/Hardware – Including but not limited to maintaining an Inventory of hardware/software within the environment helps to identify vulnerable aspects left open to threat vectors without performing vulnerability scans and to have specific knowledge of what is within the system's environment.
    f. Account Management- Including but not limited to the determination of who/what has access to the system's environment and data and also maintain access controls to the system.

g. Configuration Management – Including but not limited to defining the baseline configurations of the servers and endpoints of a system to mitigate threat factors that can be utilized to gain access to the system/data.

h. Incident Response – Including but not limited to the ability to detect security events, investigate, and mitigate or limit the effects of those events.

i. Governance and Privacy Compliance Program – Including but not limited to appointing a responsible official to develop and implement operational privacy compliance policies for information systems and databases.

j. Privacy Impact/Risk Assessment – Including but not limited to appointing a responsible official to develop and implement a formal policy and procedures to assess the organizations risk posture.

k. Awareness and Training Program – Including but not limited to appointing a responsible official to develop and implement security and privacy education awareness program for all staff members and contractors.

l. Data Retention and Destruction – Including but not limited to developing formal policy and procedures for data retention and destruction of PII.

c. PII Received. Subject to the terms and conditions of this Agreement and applicable laws, in performing the tasks contemplated under this Agreement, WBE may create, collect, disclose, access, maintain, store, and use the following PII from Consumers, Applicants, Qualified Individuals, or Enrollees, 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 Children's Health Insurance Program 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 CSR eligibility indicator, start and end dates
Applicant CSR level
Applicant QHP eligibility status change
Applicant APTC eligibility status change
Applicant CSR 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
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
Dependent name
Applicant/dependent sex
Student status
Subscriber indicator and relationship to subscriber
Total individual responsibility amount

d. Collection of PII. PII collected from Consumers, Applicants, Qualified Individuals, Enrollees—or their legal representatives or Authorized Representatives—in the context of completing an application for QHP, APTC, or CSR eligibility, or any data transmitted from or through the Hub, may be used only for Authorized Functions specified in Section II.a of this Agreement. Such information may not be used for purposes other than authorized by this agreement or as consented to by a Consumer, Applicant, Qualified Individual, or Enrollee.

e. Collection and Use of Information Provided Under Other Authorities. This

Agreement does not preclude WBE from collecting information from Consumers, Applicants, Qualified Individuals, or Enrollees—or their legal representatives or Authorized Representative—for a non-FFE/non-SBE-FP/non-Hub purpose, and using, reusing, and disclosing the non-FFE/non-SBE-FP/non-Hub information obtained as permitted by applicable law and/or other applicable authorities. Such information must be stored separately from any PII collected in accordance with Section II.c of this Agreement.

f. Ability of Individuals to Limit Collection and Use. WBE agrees to allow the Consumer, Applicant, Qualified Individual, or Enrollee to limit WBE's creation, collection, disclosure, access, maintenance, storage, and use of their PII to the sole purpose of obtaining WBE's assistance in applying for a QHP, APTC or CSR eligibility, and for performing Authorized Functions specified in Section II.a of this Agreement.

g. Incident and Breach Reporting. WBE agrees to report any suspected or confirmed 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 of the Incident or Breach. In the event of an Incident or Breach WBE must permit CMS to gather all information necessary to conduct all Incident response activities deemed necessary by CMS. If WBE fails to report an Incident or Breach in compliance with this provision, the WBE may be subject to the Termination provision (Section IV) of this Agreement. Termination pursuant to Section IV may also result where an Incident or Breach is found to have resulted from WBE's failure to comply with the terms of this Agreement.

III. Effective Date and Term; Renewal.

a. Effective Date and Term. This Agreement becomes effective on the date the last of the two Parties executes this Agreement and ends the day before the first day of the open enrollment period for the benefit year beginning January 1, 2018.

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 WBE.

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.

b. Termination with Cause. The termination of this Agreement shall be governed by the termination standards adopted by the FFE or SBE-FP under 45 CFR 155.220. Notwithstanding the foregoing, WBE shall be considered in "Habitual Default" of this Agreement if it has been served with a thirty (30)-Day notice under 45 CFR

155.220 more than three (3) times in any calendar year, whereupon CMS may, in its sole discretion, immediately thereafter terminate this Agreement upon notice to WBE without any further opportunity to cure or propose cure. CMS may also temporarily suspend the ability of a WBE to make its website available to transact information with HHS pursuant to 45 CFR 155.220(c)(4)(ii).

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

d. Destruction of PII. WBE 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, WBE has in its possession PII for which no retention period is specified in Appendix A, such PII shall be destroyed within thirty (30) Days of the termination or expiration of this Agreement. The WBE'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.

e. De-registration from the FFEs. WBE acknowledges that the termination or expiration of this Agreement may result in the de-registration of WBE from the FFEs and SBE-FPs.

V. 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

If to WBE, to WBE's address on record.

Notices sent by hand or overnight courier service, 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; provided, that 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. A Party to this Agreement may change its contact information for notices and other communications by providing thirty (30)-Days' written notice of such change in accordance with this provision.

b. Assignment and Subcontracting. WBE 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 WBE 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' sole and absolute discretion. WBE further shall not assign this Agreement or any of its rights or obligations hereunder without the prior written consent of the State. If WBE 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 WBE shall remain legally bound hereto and responsible for all obligations under this Agreement. WBE shall further be thereafter subject to such compliance actions as may otherwise be provided for under applicable law.

c. Use of the FFM Web Services. WBE will only use a CMS-approved Direct Enrollment pathway to facilitate enrollment through the FFEs and SBE-FPs.

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

e. 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.

f. Disclaimer of Joint Venture. Neither this Agreement nor the activities of WBE contemplated by and under this Agreement shall be deemed or construed to create in any way any partnership, joint venture or agency relationship between CMS and WBE. 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 ACA and the

regulations codified thereunder, including as codified at 45 CFR part 155.

g. 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.

h. Compliance with Law. WBE 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.

i. Governing Law. 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 by HHS or any of its constituent agencies, without regard to any conflict of laws statutes or rules. WBE 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*.

j. 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 WBE ("CMS notice period") unless circumstances warrant an earlier effective date. Any amendments made under this provision will only have prospective effect and will not be applied retrospectively. WBE 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.

k. Audit and Compliance Review. WBE agrees that CMS, the Comptroller General, the Office of the Inspector General of HHS, or their designees may conduct compliance reviews or audits, which includes the right to interview employees, contractors and business partners of the WBE and to audit, inspect, evaluate, examine, and make excerpts, transcripts, and copies of any books, records, documents, and other evidence of WBE's compliance with the requirements of this Agreement upon reasonable notice to WBE, during WBE's regular business hours, and at WBE's regular business location. These audit and review rights

include the right to audit WBE's compliance with and implementation of the privacy and security requirements under this Agreement. WBE further agrees to allow reasonable access to the information and facilities, including but not limited to WBE website testing environments, requested by CMS, the Comptroller General, the Office of the Inspector General of HHS, or their designees for the purpose of such a compliance review or audit. CMS may suspend or terminate the agreement of a WBE that does not comply with such a compliance review request within seven business days.

l. APTC Selection and Attestation. WBE must allow Consumers, Applicants, Qualified Individuals, and Enrollees to select and attest to an APTC amount, if applicable, in accordance with 45 CFR 155.310(d)(2). WBE should use the specific language detailed the FFM and FF-SHOP Enrollment Manual, available at https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Updated_Enrollment_Operations_Policy-and_Guidance_Final_9-30-2015_mb.pdf, when providing consumers with the ability to attest to an APTC amount.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

This "Agreement between WBE and the Centers for Medicare & Medicaid Services for the Federally-facilitated Exchange Individual Market" has been signed and executed by:

FOR WBE

The undersigned is an authorized official of WBE who is authorized to represent and bind WBE for purposes of this Agreement.

10-7-16

Signature of Authorized Official of WBE — Date

Tom Tsao, Executive Vice President & Chief Techology and Product Officer

Printed Name and Title of Authorized Official of WBE

eHealthInsurance Services, Inc.

WBE Name

Signature of Privacy Officer Attesting Compliance that WBE Systems Comply with the Critical Privacy and Security Controls under Section II.b.3 of the Agreement

Emily Lee, Privacy Officer and Associate General Counsel

Printed Name and Title of Privacy Officer Attesting Compliance that WBE Systems Comply with the Critical Privacy and Security Controls under Section II.b.3 of the Agreement

eHealthInsurance Services, Inc.

440 East Middlefield Road

Mountain View, California 94043

WBE Address

John Desser, VP Government Affairs / Public Policy

(202) 506-1096

WBE Contact Number

FOR CMS

The undersigned are officials of CMS who are authorized to represent CMS for purposes of this Agreement.

Karen Shields

Karen Shields
Deputy Director, Operations
Center for Consumer Information & Insurance Oversight
Centers for Medicare & Medicaid Services

10-21-16

Date

George C. Hoffmann

George C. Hoffmann
Acting Chief Information Officer
Centers for Medicare & Medicaid Services

10/26/16

Date

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 ("ACA") (42 U.S.C. § 18081(g)), the Federal Information Management Act of 2002 ("FISMA") (44 U.S.C. 3541), and 45 CFR 155.260. All capitalized terms used herein carry the meanings assigned in Appendix B, "Definitions." Any capitalized term that is not defined in Appendix B has the meaning provided in 45 CFR 155.20.

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).

The FFEs will enter into contractual agreements with all Non-Exchange Entities, including WBE that gain access to Personally Identifiable Information ("PII") exchanged with the FFEs and SBE-FPs, or directly from Consumers, Applicants, Qualified Individuals, or 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 the FFEs and SBE-FPs. 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 FFE under 155.260(a)(3) and as applicable to non-Exchange entities under 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 FFE, 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: Individual Access to PII. 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 the 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, 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 their 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 thirty (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; or
    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, 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 website, 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 timely and accessible 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; and
    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 website, 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 website.

(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, 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 the 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); and
   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 ten (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, or Qualified Employer.*

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:

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 not, to the greatest extent practicable, collect PII directly from the Consumer, Applicant, Qualified Individual, or Enrollee, when the information is likely to 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 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, 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 PII 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 by telephone. They may also be offered an opportunity to meet with the Responsible Official 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; and
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) 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 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, 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 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. In keeping with the standards and implementation specifications used by the FFE, Non-Exchange Entities should adopt and implement the standards and implementation specifications in this document 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 incorporate these procedures in the Non-Exchange Entity's own written policies and procedures.

i. Implementation Specifications. Such policies and procedures would:

1. 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;
2. 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.
3. Require reporting of 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 after discovery of the Incident or Breach.

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.

[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

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.

ANNUAL SECURITY AND PRIVACY ATTESTATION (SPA)

The Non-Exchange Entity shall complete an annual SPA assessment as described below. The SPA assessment shall include the following:

- Documentation of existing security and privacy controls;
- Identification of potential security and privacy risks; and
- Corrective action plan describing approach and timeline to implement security and privacy controls to mitigate potential security and privacy risks.

(1) Assessment Options. The following options are acceptable approaches for completing the SPA assessment:

a. The Non-Exchange Entity may contract with a third party with experience conducting information system privacy and security audits to perform the SPA assessment.

b. The Non-Exchange Entity may utilize internal information system staff resources to perform the SPA assessment, provided such staff have no direct responsibility for the security or privacy posture of the information system that is the subject of the SPA assessment.

c. The Non-Exchange Entity may reference existing audit results that address some or all of the SPA assessment's requirements. Such existing audit results must have been generated using one of the methods described above in the first two assessment options. In addition, such existing audit results must have been produced within 365 days of completion of the SPA assessment. If existing audit reports do not address all

required elements of the SPA assessment, the remaining elements must be addressed utilizing one of the first two assessment options.

(2) Assessment Methodology. The SPA assessment methodology described herein is based on the standard CMS methodology used in the assessment of all CMS internal and business partner information systems. The Non-Exchange Entity shall prepare an assessment plan to evaluate any system vulnerabilities. The assessment methods may include examination of documentation, logs, and configurations; interviews of personnel; and/or testing of technical controls. The SPA assessment shall provide an accurate depiction of the security and privacy controls in place, as well as potential security and privacy risks, by identifying the following:

a. Application or system vulnerabilities, the associated business and system risks and potential impact;

b. Weaknesses in the configuration management process such as weak system configuration settings that may compromise the confidentiality, integrity, and availability of the system;

c. Non-Exchange Entity security and privacy policies and procedures; and

d. Major documentation omissions and/or discrepancies.

(3) Tests and Analysis Performed. The SPA assessment may include tests that analyze applications, systems, and associated infrastructure. The tests may begin with high-level analyses and increase in specificity. Tests and analyses performed during an assessment may include:

a. Security control technical testing;

b. Adherence to privacy program policies;

c. Network and component scanning;

d. Configuration assessment;

e. Documentation review;

f. Personnel interviews; and

g. Observations.

(4) Noncompliance and Applicability. The Non-Exchange Entity must develop a corrective action plan to mitigate any security and privacy risks if the SPA assessment identifies a deficiency in the Non-Exchange Entity's security and privacy controls. Alternatively, the Non-Exchange Entity may document why it believes a critical control is not applicable to its system or circumstances. The SPA assessment results do not alter the Agreement between the Non-Exchange Entity and CMS, including any penalties for non-compliance. If the Non-Exchange Entity's SPA assessment includes findings suggesting significant security or privacy risks, and the Non-Exchange Entity does not commence development and implementation of a corrective action plan to the reasonable satisfaction of CMS, a comprehensive audit may be initiated by CMS, and/or the Agreement between the Non-Exchange Entity and CMS may be terminated for cause.

(5) Critical Security and Privacy Controls. The critical controls the Non-Exchange Entity must

evaluate on an annual basis are:

a. Email/Web Browser Protections – Including but not limited to assurance that transfer protocols are secure and limits the threat of communications being intercepted.

b. Malware Protection – Including but not limited to protections against known threat vectors within the system's environment to mitigate damage/security breaches.

c. Patch Management – Including but not limited to ensuring every client and server is up to date with the latest security patches throughout the environment.

d. Vulnerability Management – Including but not limited to identifying, classifying, remediating, and mitigating vulnerabilities on a continual basis by conducting periodic vulnerability scans to identify weaknesses within an environment.

e. Inventory of Software/Hardware – Including but not limited to maintaining an Inventory of hardware/software within the environment helps to identify vulnerable aspects left open to threat vectors without performing vulnerability scans and to have specific knowledge of what is within the system's environment.

f. Account Management- Including but not limited to the determination of who/what has access to the system's environment and data and also maintain access controls to the system.

g. Configuration Management – Including but not limited to defining the baseline configurations of the servers and endpoints of a system to mitigate threat factors that can be utilized to gain access to the system/data.

h. Incident Response – Including but not limited to the ability to detect security events, investigate, and mitigate or limit the effects of those events.

i. Governance and Privacy Compliance Program – Including but not limited to appointing a responsible official to develop and implement operational privacy compliance policies for information systems and databases.

j. Privacy Impact/Risk Assessment – Including but not limited to appointing a responsible official to develop and implement a formal policy and procedures to assess the organizations risk posture.

k. Awareness and Training Program – Including but not limited to appointing a responsible official to develop and implement security and privacy education awareness program for all staff members and contractors.

l. Data Retention and Destruction – Including but not limited to developing formal policy and procedures for data retention and destruction of PII.

(6) National Institute for Standards and Technology Special Publication 800-53, Revision 4 (NIST SP 800-53, Rev. 4). Third party verification and documentation of the Non-Exchange Entity's compliance with some or all of NIST SP 800-53, Rev. 4 that correspond to the critical controls listed above shall be accepted by CMS as documentation of compliance with those critical controls.

(7) SPA Format. The template provided in Appendix D must be used to document completion

of the annual SPA assessment. The signatories on the SPA personally attest to its accuracy and authenticity.

(8) Submission of SPA to CMS. The SPA must be submitted electronically in a format specified by CMS or by mail to CMS at the address in Section V above by July 1, 2017.

(9) CMS Verification of SPA. CMS will review the Non-Exchange Entity's SPA assessment, and for any critical security or privacy control that the Non-Exchange Entity claimed as not applicable, CMS, in its sole discretion, will determine if the claim is justified. If CMS determines such controls are applicable, CMS may require a supplementary assessment of such controls and an amended SPA submission from the Non-Exchange Entity. If the SPA assessment indicates that the Non-Exchange Entity does not meet any critical control, CMS may require remedial action. A Non-Exchange Entity that does not complete a SPA assessment or any required supplemental assessment or remedial actions may be subject to the Termination with Cause provision (Section IV, b) of this agreement.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

APPENDIX B

DEFINITIONS

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

(1) **Affordable Care Act (ACA)** 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 Affordable Care Act.

(2) **Access** means availability of a SORN Record to a Subject Individual.

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

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

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

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

(7) **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.

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

(9) **Breach** is defined by OMB Memorandum M-07-16, Safeguarding and Responding to the Breach of Personally Identifiable Information (May 22, 2007), as the compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, loss of control or any similar term or phrase that refers to situations where persons other than authorized users or for an other than authorized purpose have access or potential access to Personally Identifiable Information (PII), whether physical or electronic.

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

(11) **Certified Application Counselor** means an organization, staff person, or volunteer meeting the requirements set forth in 45 CFR 155.225.

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

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

(14) **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.

(15) **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 Federally-facilitated Exchange website, including the collection of personal and financial information necessary for Consumer, Applicant, Qualified Individual, Qualified Employer, Qualified Employee, or Enrollee account creations; Qualified Health Plan (QHP) application submissions; and Insurance Affordability Program eligibility determinations.

(16) **Consumer** means a person who, for himself or herself, or on behalf of another individual, seeks information related to eligibility or coverage through a Qualified Health Plan (QHP) or Insurance Affordability Program, or whom an agent or broker (including Web-brokers) registered with the applicable FFE, Navigator, Issuer, Certified Application Counselor, or other entity assists in applying for a QHP, applying for APTCs and CSRs, and/or completing enrollment in a QHP through an FFE for individual market coverage.

(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, or Qualified Individual including but not limited to responding to questions and complaints and providing information about Health Insurance Coverage and enrollment processes in connection with the FFEs.

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

(20) **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.

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

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

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

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

(25) **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).

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

(27) **Health Insurance Exchanges Program (HIX)** means the System of Records that CMS uses in the administration of the FFE. 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 FR 8538 (February 6, 2013), and amended by 78 FR 32256 (May 29, 2013) and 78 FR 63211 (October 23, 2013).

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

(29) **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.

(30) **Incident**, or **Security Incident**, means the act of violating an explicit or implied security policy, which includes attempts to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

(31) **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.

(32) **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 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 available to Qualified Individuals.

(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 Affordable Care Act.

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

(34) **Non-Exchange Entity** has the meaning at 45 CFR 155.260(b)(1), including, but not limited to QHP issuers, Navigators, Agents, and Brokers.

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

(36) **Personally Identifiable Information (PII)** has the meaning contained in OMB Memoranda M-07-16 (May 22, 2007) and means information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth and mother's maiden name.

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

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

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

(40) **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.

(41) **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.

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

(43) **State-based Exchange on the Federal Platform (SBE-FP)** means an Exchange 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.

(44) **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.

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

(46) **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.

(47) **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.

(48) **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 the 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.

(49) **Web-broker** means an agent or broker who uses a non-Federally-facilitated Exchange Internet website to assist Consumers, Applicants, Qualified Individuals, and Enrollees in the QHP selection and enrollment process as described in 45 CFR 155.220(c).

(50) **Web-Based Entity** means a Non-Exchange Entity that performs direct enrollment under this agreement.

(51) **Workforce** means a Non-Exchange Entity's or FFE'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.

APPENDIX C

STANDARDS FOR COMMUNICATION WITH THE HUB

(1) Web-based Entity ("WBE") must complete testing for each Hub-related transaction it will implement, and shall not be allowed to exchange data with CMS in production mode until testing is satisfactorily passed, as determined by CMS in its sole discretion. Successful testing generally means the ability to pass all applicable HIPAA compliance standards, or other CMS-approved standards, and to process electronic data and information transmitted by WBE to the Hub. The capability to submit these test transactions will be maintained by WBE throughout the term of this Agreement.

(2) Transactions must be formatted in accordance with the Accredited Standards Committee Implementation Guides adopted under HIPAA, available at http://store.x12.org/store/, as applicable and appropriate for the type of transaction. CMS will make available Companion Guides for the transactions, which specify necessary situational data elements.

(3) WBE agrees to abide by the applicable policies affecting electronic data interchange submissions and submitters as published in any of the guidance documents related to the CMS FFE or Hub, as well as applicable standards in the appropriate CMS Manual(s) or CMS Companion Guide(s), as published on the CMS website. These materials can be found at http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/companion-guide-for-ffe-enrollment-transaction-v15.pdf and http://www.cms.gov/cciio/resources/regulations-and-guidance/index.html.

(4) WBE agrees to submit test transactions to the Hub prior to the submission of any transactions to the FFE production system and to determine that the transactions and responses comply with all requirements and specifications approved by the CMS and/or the CMS contractor.[2]

(5) WBE agrees that prior to the submission of any additional transaction types to the FFE production system, or as a result of making changes to an existing transaction type or system, it will submit test transactions to the Hub in accordance with paragraph (1) above.

(6) If WBE enters into relationships with other affiliated entities, or their authorized designees for submitting and receiving FFE data, it must execute contracts with such entities stipulating that that such entities and any of its subcontractors or affiliates must utilize software tested and approved by WBE as being in the

[2] While CMS owns data in the FFE, contractors operate the FFE system in which the enrollment and financial management data flow. Contractors provide the pipeline network for the transmission of electronic data, including the transport of Exchange data to and from the Hub and WBE so that WBE may discern the activity related to enrollment functions of persons they serve. WBE may also use the transported data to receive descriptions of financial transactions from CMS.

proper format and compatible with the FFE system. Entities that enter into contract with WBE and access PII are required to maintain the same or more stringent security and privacy controls as WBE.

(7) WBE agrees that CMS may require successful completion of an Operational Readiness Review to the satisfaction of CMS, which may occur before WBE is able to submit any transactions to the FFE production system or at any time during the term of this Agreement. The Operational Readiness Review will assess WBE's compliance with CMS' regulatory and contractual requirements, to include the critical privacy and security controls. This Agreement may be terminated or access to CMS systems may be denied for a failure to comply with Operational Readiness Review or if, at the sole discretion of CMS, the results are unsatisfactory. WBE must attest that its systems are in compliance with applicable critical privacy and security controls under Section II.b.3 of the Agreement as a condition of executing this agreement.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

APPENDIX D

Annual Security and Privacy Attestation Report – *Web-Based Entity*

Self-Attestation for Year: (e.g. January 2017 – December 2017)
Date Completed:

Attestation Identification	
Web-Based Entity	
System Name	
Business Owner	
Security Officer	
Privacy Officer	

Critical Control	Met	Not Met	N/A	Date (Day/Month/Year)
1. Email/Web Browser Protections: Including but not limited to assurance that transfer protocols are secure and limits the threat of communications being intercepted.				
2. Malware Protection: Including but not limited to protections against known threat vectors within the system's environment to mitigate damage/security breaches.				
3. Patch Management: Including but not limited to ensuring every client and server is up to date with the latest security patches throughout the environment.				
4. Vulnerability Management: Including but not limited to identifying, classifying, remediating, and mitigating vulnerabilities on a continual basis by conducting periodic vulnerability scans to identify weaknesses within an environment.				
5. Inventory of Software/Hardware: Including but not limited to maintaining an Inventory of hardware/software within the environment helps to identify vulnerable aspects left open to threat vectors without performing vulnerability scans and to have specific knowledge of what is within the system's environment.				
6. Account Management: Including but not limited to the determination of who/what has access to the system's environment and data				

Critical Control	Met	Not Met	N/A	Date (Day/Month/Year)
and also maintain access controls to the system.				
7. Configuration Management: Including but not limited to defining the baseline configurations of the servers and endpoints of a system to mitigate threat factors that can be utilized to gain access to the system/data.				
8. Incident Response: Including but not limited to the ability to detect security events, investigate, and mitigate or limit the effects of those events.				
9. Governance and Privacy Compliance Program: Including but not limited to appointing a responsible official to develop and implement operational privacy compliance policies for information systems and databases.				
10. Privacy Impact/Risk Assessment: Including but not limited to appointing a responsible official to develop and implement a formal policy and procedures to assess the organizations risk posture.				
11. Awareness and Training Program: Including but not limited to appointing a responsible official to develop and implement security and privacy education awareness program for all staff members and contractors.				
12. Data Retention and Destruction: Including but not limited to developing formal policy and procedures for data retention and destruction of PII.				

Explanation for any critical control not met or not applicable (use additional pages if necessary):

Self- Attestation for Year:
(e.g., January 2017 – December 2017)
Date Completed:

System Security Officer

Signature Date

Privacy Officer

Signature Date

Business Owner

Signature Date

Please read the following Agreement carefully. By clicking "I Agree" when this option is made available to you, you understand this constitutes your electronic signature and you accept/agree to be bound by and abide by the terms and conditions of the Agreement. If you do not want to accept/agree to the terms and conditions of the Agreement, you must click "I Do Not Agree."

AGENT BROKER GENERAL AGREEMENT FOR INDIVIDUAL MARKET FEDERALLY-FACILITATED EXCHANGES AND STATE-BASED EXCHANGES ON THE FEDERAL PLATFORM

THIS AGENT BROKER GENERAL AGREEMENT ("Agreement") is entered into between the agent, broker, or entity who established this account and whose name appears on the Marketplace Learning Management System (MLMS) account ("AB") and the Centers for Medicare & Medicaid Services ("CMS"), the entity responsible for the management and oversight of the Federally-facilitated Exchange ("FFE") and the Federal eligibility and enrollment platform upon which certain State-based Exchanges rely for eligibility and enrollment functionality (SBE-FPs), pursuant to Section 1312(e) of the Affordable Care Act ("ACA") and the regulations promulgated thereunder, as codified in 45 CFR 155.220(d).

I. BACKGROUND

Section 1312(e) of the ACA provides that the Secretary of the U.S. Department of Health and Human Services shall establish procedures under which Agents or Brokers may participate in an Exchange. 45 CFR 155.220 provides that Agents and Brokers may enroll individuals in a Qualified Health Plan ("QHP") as soon as the QHP is offered through an Exchange in the State; and may also assist individuals in applying for enrollment in a QHP through the Exchange, Advance Payments of the Premium Tax Credits ("APTCs") and/or Cost-Sharing Reductions ("CSRs"), to the extent that Agents and Brokers are permitted to do so by the State in which they operate.

45 CFR 155.220(d) requires all Agents or Brokers enrolling Qualified Individuals in QHPs in a manner that constitutes enrollment through the Exchange, or assisting Qualified Individuals in applying for QHPs, APTCs and CSRs, to comply with the terms of an agreement between the Agent or Broker and the Exchange.

Pursuant to section 155.220(d) and subject to State law, this Agreement establishes the standards and requirements for AB to: (a) assist Consumers, Applicants, Qualified Individuals, and Enrollees in applying for eligibility for QHPs, APTCs, and/or CSRs; and (b) enroll Qualified Individuals in a QHP through the individual market FFEs and SBE-FPs in a manner that constitutes enrollment through an Exchange.

II. DEFINITIONS

Terms in this paragraph are defined pursuant to federal regulations, and are subject to change through future rulemaking.

a. *Agent or broker*: Has the meaning set forth in 45 CFR 155.20.

b. *Advance Payments of the Premium Tax Credit (APTC)*: Has the meaning set forth in 45 CFR 155.20.

c. *Applicant*: Has the meaning set forth in 45 CFR 155.20.

d. *Cost-sharing Reduction (CSR)*: Has the meaning set forth in 45 CFR 155.20.

e. *Consumer*: A person who, for himself or herself, or on behalf of another individual, seeks information related to eligibility or coverage through a Qualified Health Plan (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 APTCs and CSRs, and/or completing enrollment in a QHP through its web site for individual market coverage.

f. *Enrollee*: As defined for the purposes of this Agreement, an individual enrolled in a QHP or other Insurance Affordability Program.

g. *Federally-facilitated Exchange (FFE)*: As defined for the purposes of this Agreement, an Exchange established by HHS and operated by CMS under Section 1321(c)(1) of the Affordable Care Act for individual market coverage.

h. *Insurance Affordability Program*: 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 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 available to Qualified Individuals.

(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 Affordable Care Act.

i. *Personally Identifiable Information (PII):* Has the meaning contained in OMB Memoranda M-07-16 (May 22, 2007) and means information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

j. *Qualified Health Plan (QHP)*: Has the meaning set forth in 45 CFR 155.20.

k. *Qualified Individual*: Has the meaning set forth in 45 CFR 155.20.

l. *State-based Exchange on the Federal platform (SBE-FP):* As defined for purpose of this Agreement, an Exchange 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.

III. OBLIGATIONS AND CONDITIONS

To enroll Qualified Individuals in a QHP in a manner that constitutes enrollment through the FFE or SBE-FP and to assist individuals in applying for APTCs and CSRs, AB hereby agrees to:

a. Register with the FFE in advance of assisting Consumers, Applicants, Qualified Individuals, and Enrollees, or enrolling Qualified Individuals in QHPs through the FFE or SBE-FP;

b. Receive training in the range of QHP options and insurance affordability programs offered through the FFE or SBE-FP;

c. Comply with the privacy and security standards adopted by the FFE as a condition of a separately executed agreement with CMS pursuant to 45 CFR 155.260(b);

d. Comply with all applicable State law related to Agents and Brokers in each state in which AB operates, including but not limited to State laws related to confidentiality and conflicts of interest; and State laws related to appointments, as a condition of enrolling Consumers, Applicants, Qualified Individuals, and Enrollees in QHPs through the FFE or SBE-FP;

COPY

e. Maintain valid licensure in every state that AB assists Consumers, Applicants, Qualified Individuals, and Enrollees in applying for or obtaining coverage under a QHP through an FFE or SBE-FP;

f. Comply with the Affordable Care Act and all applicable current and future regulations and guidance; and

g. Comply with any and all other 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 the Health Insurance Portability and Accountability Act (HIPAA); Section 6103(b)(2) of the Internal Revenue Code; 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 statutory, regulatory, or sub-regulatory guidance released by CMS shall control.

IV. MISCELLANEOUS

a. Effective Date, Term and Renewal. This Agreement becomes effective on the date that AB 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, 2018. This Agreement is renewable for subsequent one (1)-year terms upon thirty (30) Days' advance written notice to AB at CMS's sole and absolute discretion.

b. Termination and Reconsideration.
   i. The termination of this Agreement and the reconsideration of any such termination shall be governed by the termination and reconsideration standards adopted by the FFE under 45 CFR 155.220.
   ii. Termination for Failure to Maintain Valid State Licensure. AB acknowledges and agrees that valid state licensure in each state in which AB assists Consumers, Applicants, Qualified Individuals, and Enrollees in applying for or obtaining coverage under a QHP through an FFE or SBE-FP is a condition to AB's authority under this Agreement. Accordingly, CMS may terminate this Agreement upon thirty (30) Days' prior written notice if AB 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 FFE under 45 CFR 155.220(g).

c. 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

If to AB, to AB's address on record.

Notices sent by hand or overnight courier service, 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; provided, that 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. CMS and AB may change their contact information for notices and other communications by providing thirty (30) Days' written notice of such change in accordance with this provision.

d. Assignment and Subcontracting. AB 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 AB 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. AB further shall not assign this Agreement or any of its rights or obligations hereunder without the prior written consent of CMS. If AB 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 AB shall remain legally bound hereto and responsible for all obligations under this Agreement. AB shall further be thereafter subject to such compliance actions as may otherwise be provided for under applicable law.

e. 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.

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

g. 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.

h. Governing Law. This Agreement shall 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 the HHS or any of its constituent agencies, without regard to any conflict of laws statutes or rules. AB 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. AB acknowledges that during the term of this Agreement, CMS may amend this Agreement to incorporate any additional standards required by statute, regulation or policy implementing or interpreting such statutory or regulatory provisions. Notwithstanding the foregoing, should there be any conflict or inconsistency between the standards and obligations contained in this Agreement and any statutory, regulatory, or sub-regulatory guidance released by CMS, AB must comply with the statutory, regulatory, and sub-regulatory standards released by CMS.

Accept Agreement

Do you accept the terms and conditions of the Agent Broker General Agreement for the Federally-facilitated Exchange and/or State-based Exchange on the Federal Platform Individual Market?

Select "I Agree" to provide your electronic signature.

Select your response and then click **Submit**.

- (•) I Agree
- ( ) I Do Not Agree

Correct Answer:
You have accepted the terms and conditions of the Agent Broker General Agreement for the Federally-facilitated Exchange and/or State-based Exchange on the Federal Platform Individual Market. Your records will be updated accordingly to reflect your electronic signature.

Incorrect Answer:
You have not accepted the terms and conditions of the Agent Broker General Agreement for the Federally-facilitated Exchange and/or State-based Exchange on the Federal Platform Individual Market. As a result, you will not be permitted to register as an agent or broker in the Federally-facilitated Marketplaces or the State-based Marketplace on the Federal Platform for the individual market.

Please carefully read the following Agreement and Appendices, which are incorporated by reference into the Agreement. By clicking "I Agree" when this option is made available to you, you understand this constitutes your electronic signature and you accept/agree to be bound by and abide by the terms and conditions of the Agreement. If you do not want to accept/agree to the terms and conditions of the Agreement, you must click "I Do Not Agree".

You can access the Appendices to this Agreement by clicking on the following links:

Appendix A

Appendix B

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 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 Credits ("APTCs") 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 equates to the Federally-facilitated Marketplaces*

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

WHEREAS:

1. Section 1312(e) of the Affordable Care Act ("ACA") 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 Advance Payments of the Premium Tax Credit ("APTCs") and Cost-sharing Reductions ("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 their 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 ACA and implementing regulations permit.

3. ABE is an entity or individual licensed by the applicable State Department of Insurance ("DOI") in at least one FFM or SBM-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 Sections 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 156.260(a)(1) through (a)(6), including being at least as protective as the standards the Exchange has established and implemented for itself under 45 CFR 155.260(a)(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 the attached 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," which is incorporated by reference in this Agreement, while engaging in any activity as an Agent or Broker for purposes of the facilitating enrollment through the FFEs or SBE-FPs. ABE shall be bound to 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 adhere to the same.

a. Authorized Functions. ABE may create, collect, disclose, access, maintain, store, and use PII 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 APTCs or CSRs, and selecting an APTC amount;
4. Facilitating the collection of standardized attestations acknowledging the receipt of the APTC or CSR 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 CSR and APTC information to the FFEs or SBE-FPs;
8. Facilitating payment of the initial premium amount to appropriate QHP;
9. Facilitating an Enrollee's ability to disenroll from a QHP; and
10. Educating Consumers, Applicants, 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 the 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, when Enrollees may no longer be eligible to maintain their current QHP coverage because of age, or to inform Enrollees of coverage QHP 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 shall may be approved by CMS in writing from time to time.

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 CSR eligibility indicator, start and end dates
- Applicant CSR level
- Applicant QHP eligibility status change
- Applicant APTC eligibility status change
- Applicant CSR 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
- 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 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 CSR 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 CSR eligibility, and for performing 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, 2018.

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 FFE 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 qualified health plan through an FFE or SBE-FP is a precondition 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 FFE 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

If to ABE, to ABE'S address on record.

Notices sent by hand or overnight courier service, 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; provided, that 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 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 ACA 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 which constitutes the stricter, higher or more stringent level of compliance shall control.

h. Governing Law. 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.

Accept Privacy and Security Agreement

Do you agree to accept the privacy and security terms and conditions of the Agreement between Agent or Broker and CMS for the Federally-facilitated Exchange and State-Based Exchange on the Federal Platform **Individual Market?**

Select "I Agree" to provide your electronic signature.

Select your response and then click **Submit**. After you have submitted your response, please close the window by clicking **'Exit'** in the upper right corner. This will ensure that your response is entered successfully.

- ○ I Agree
- ○ I Do Not Agree

Correct Answer:
You have accepted the terms and conditions of the Agreement between Agent or Broker and CMS for the Federally-facilitated Exchange and State-Based Exchange on the Federal Platform Individual Market. Your records will be updated accordingly to reflect your electronic signature.

Incorrect Answer:
You have not accepted the terms and conditions of the Agreement between Agent or Broker and CMS for the Federally-facilitated Exchange and the State-based Exchange on the Federal Platform Individual Market. As a result, you will not be registered as an agent or broker in the Federally-facilitated Marketplaces or the State-based Marketplaces on the Federal Platform for the Individual Marketplace.

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. Capitalized terms not otherwise specifically defined herein shall have the meaning assigned in Appendix B, "Definitions." If the term isn't 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, Enrollees, Qualified Employees, and Qualified Employers, 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 155.260(a)(3) and as applicable to non-Exchange entities under 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 FFE, Non-Exchange Entities that maintain and/or store PII must provide Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, 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 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, 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 their 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.

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 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.

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 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, 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 the 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 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, or Qualified Employer.*

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:

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 above 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, 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 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 FFEs and SBE-FPs, Non-Exchange Entities must offer Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, 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 10 working days of receipt.

4. If the Non-Exchange Entity (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 Non-Exchange Entity (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, 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. In keeping with the standards and implementation specifications used by the FFE, Non-Exchange Entities should adopt and implement the privacy and security standards as established by the FFE under 155.260(a)(3) and as applicable to non-Exchange entities under 155.260(b)(3), 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 functions involving the creation, collection, disclosure, access, maintenance, storage, or use of PII.

i. Implementation Specifications:

[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

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 FFE is sufficient to satisfy the requirements of this paragraph.

(7) *Safeguarding PII. In keeping with the standards and implementation specifications used by the FFE, 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 Appendices that are not defined therein and not defined here has the meaning provided in 45 CFR 155.20.

(1) **Affordable Care Act (ACA)** 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 Affordable Care Act.

(2) **Access** means availability of a SORN Record to a subject individual.

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

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

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

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

(7) **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.

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

(9) **Breach** is defined by OMB Memorandum M-07-16, Safeguarding and Responding to the Breach of Personally Identifiable Information (May 22, 2007), as the compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, loss of control or any similar term or phrase that refers to situations where persons other than authorized users or for an other than authorized purpose have access or potential access to Personally Identifiable Information (PII), whether physical or electronic.

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

(11) **Certified Application Counselor** means an organization, staff person, or volunteer meeting the requirements set forth in 45 CFR 155.225.

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

(13) **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.

(14) **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.

(15) **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 Federally-facilitated Exchange or State-based Exchange on the Federal Platform website, including the collection of personal and financial information necessary for Consumer, Applicant, Qualified Individual, Qualified Employer, Qualified Employee, or Enrollee account creations; Qualified Health Plan (QHP) application submissions; and Insurance Affordability Program eligibility determinations.

(16) **CMS Companion Guide** 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.

(17) **Compliance and Oversight Activities** are the routine activities and processes conducted by a QHP Issuer 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.

(18) **Consumer** means a person who, for himself or herself, or on behalf of another individual, seeks information related to eligibility or coverage through a Qualified Health Plan (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 APTCs and CSRs, and/or completing enrollment in a QHP through the Federally-facilitated Exchanges or State-based Exchanges on the Federal Platform for individual market coverage.

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

(20) **Cost-sharing Reduction (CSR)** has the meaning set forth in 45 CFR 155.20.

(21) **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.

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

(23) **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.

(24) **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.

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

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

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

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

(29) **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).

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

(31) **Health Insurance Exchanges Program (HIX)** means the System of Records that CMS uses in the administration of the FFE. 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), and amended by 78 Fed.Reg. 32256 (May 29, 2013).

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

(33) **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.

(34) **Incident**, or **Security Incident**, means the act of violating an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

(35) **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.

(36) **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 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 available to Qualified Individuals.

(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 Affordable Care Act.

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

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

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

(40) **Personally Identifiable Information (PII)** has the meaning contained in OMB Memoranda M-07-16 (May 22, 2007) and means information which can be used to distinguish or trace an individual's identity, such as their name, Social Security number, biometric records, *etc.*, alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

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

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

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

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

(45) **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.

(46) **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.

(47) **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.

(48) **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. **State-based Marketplace on the Federal Platform (SBM-FP)** has the same meaning as SBE-FP.

(49) **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.

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

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

(52) **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.

(53) **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.

(54) **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 the 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.

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

(56) **Web-broker** means an agent or broker who uses a non-Federally-facilitated Exchange internet web site to assist Consumers, Applicants, Qualified Individuals, and Enrollees in the QHP selection and enrollment process as described in 45 CFR 155.220(c).

(57) **Workforce** means a Non-Exchange Entity's, FFE's or 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.