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

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"), also referred to as "Federally-facilitated Marketplaces" or "FFMs" and the operation of the federal eligibility and enrollment platform, which includes the CMS Data Services Hub ("Hub"), relied upon by certain State-based Exchanges ("SBEs") for their eligibility and enrollment functions (including State-based Exchanges on the federal platform ["SBE-FPs"]), and_____, (hereinafter referred to as Web-broker), a Web-broker which uses a non-FFE Internet website in accordance with 45 CFR 155.220(c)(3) and 155.221 to assist Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employers, and Qualified Employees in applying for eligibility for enrollment in Qualified Health Plans ("QHPs") and for Advance Payments of the Premium Tax Credits ("APTCs") and Cost-sharing Reductions ("CSRs") for QHPs, and/or in completing enrollment in QHPs offered in the individual market through the FFEs or SBE-FPs, in applying for a determination of eligibility to participate in the FF-Small Business Health Options Program ("FF-SHOPs") or SBE-FP SHOPs and/or in completing enrollment in QHPs offered through the FF-SHOPs or SBE-FP SHOPs; and providing related Customer Service. CMS and Web-broker (hereinafter referred to as the "Party") or collectively, as the "Parties." Unless otherwise noted, the provisions of this Agreement are applicable to Web-brokers seeking to assist Qualified Employers and Qualified Employees in purchasing and enrolling in coverage through an FF-SHOP or SBE-FP SHOP.

WHEREAS:

1. Section 1312(e) of the Patient Protection and Affordable Care Act ("PPACA") provides that the Secretary of the U.S. Department of Health & Human Services ("HHS") shall establish procedures that permit Agents and Brokers to enroll Qualified Individuals in QHPs through an Exchange, and to assist individuals in applying for APTC and CSRs, to the extent allowed by States. To participate in the FFEs or SBE-FPs, including an FF-SHOP or SBE-FP SHOP, Agents, Brokers, and Web-brokers 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 application programming interfaces ("APIs") to Web-broker that will enable Web-broker to establish a secure connection with the Hub. The APIs will enable the secure transmission of key eligibility and enrollment information between CMS and Web-broker. The Hub Web Services are not available for SHOP.
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 Web-broker; (b) provide Web-broker with access to the Hub Web Services, if applicable; and (c) permit Web-broker to create, collect, disclose,

access, maintain, store, and use PII from CMS, Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals' legal representatives or Authorized Representatives—to the extent that these activities are necessary to carry out the functions that the PPACA and implementing regulations permit Web-broker to carry out. The Hub Web Services are not available for SHOP.

4. Web-broker is an individual or entity licensed as an insurance producer, agent, or broker by the applicable state regulatory authority in at least one FFE or SBE-FP state; OR Web-broker is a Direct Enrollment Technology Provider.

5. Web-broker 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, Enrollees, Qualified Employers and Qualified Employees to perform the Authorized Functions described in Section II.a of this Agreement. The Hub Web Services are not available for SHOP.

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

7. CMS has adopted privacy and security standards with which the Web-broker, a type of Non-Exchange Entity, must comply, which are set forth in Appendix A: Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities and the *Non-Exchange Entity System Security and Privacy Plan* (NEE SSP).[1]

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 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.

Web-broker and CMS are entering into this Agreement to satisfy the requirements under 45 CFR 155.260(b)(2). Web-broker 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, as applicable, which are incorporated by reference in this Agreement, while and as engaging in any activity as Web-broker for purposes of the PPACA. Web-broker shall strictly adhere to the privacy and security standards—and ensure that its employees, officers, directors, contractors, subcontractors, agents, and representatives strictly

[1] The references in this section to security and privacy controls and implementation standards can be found in the *Non-Exchange Entity System Security and Privacy Plan* (NEE SSP) located on CMS zONE at the following link: https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials.

adhere to the same—to gain and maintain access to the Hub Web Services, if applicable, and to create, collect, disclose, access, maintain, store, and use PII for the efficient operation of the FFEs and SBE-FPs.

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

1. Assisting with application, eligibility, and enrollment processes for QHP offered through the FFEs and SBE-FPs, including FF-SHOPs and SBE-FP-SHOPs;
2. Supporting QHP selection and enrollment by assisting with plan selection and plan comparisons;
3. Assisting with completing applications for the receipt of APTC or CSRs and with selecting an APTC amount, if applicable;
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, if applicable;
6. Assisting with filing appeals of eligibility determinations in connection with the FFEs and SBE-FPs, including Qualified Employer appeals for FF-SHOPs and SBE-FP-SHOPs;
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, if applicable;
8. Facilitating payment of the initial premium amount to the appropriate individual market QHP, if applicable;
9. Facilitating payment of the initial and group premium amount for FF-SHOP and SBE-FP SHOP coverage, if applicable;
10. Facilitating an Enrollee's ability to disenroll from a QHP;
11. 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");
12. Assisting Enrollees 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);
13. Handling FF-SHOP or SBE-FP SHOP coverage changes throughout the plan year that may impact eligibility, including, but not limited to, adding a new hire, removing an Employee no longer employed at the company, removing an Employee no longer employed full-time and adding a newborn or spouse during a special enrollment period, if applicable;
14. Correcting errors in the application for QHP enrollment;

15. 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;
16. Providing appropriate information, materials, and programs to Consumers, Applicants, Qualified Individuals, Enrollees, Employers, Employees, Qualified Employers, and Qualified Employees to inform and educate them about the use and management of their health information, as well as medical services and benefit options offered through the selected QHP or among the available QHP options;
17. Contacting Consumers, Applicants, Qualified Individuals, Enrollees, Employers, Employees, Qualified Employers and Qualified Employees to assess their satisfaction or resolve complaints with services provided by Web-broker in connection with the FFEs and SBE-FPs, including FF-SHOPs and SBE-FP-SHOPs, the Web-broker, or QHPs;
18. Providing assistance in communicating with QHP Issuers;
19. Providing Customer Service activities related to FF-SHOP or SBE-FP SHOP coverage if permitted under state and federal law, including correction of errors on FF-SHOP or SBE-FP SHOP applications and policies, handling complaints and appeals regarding FF-SHOP or SBE-FP SHOP coverage, responding to questions about FF-SHOP or SBE-FP insurance policies, assisting with communicating with state regulatory authorities regarding FF-SHOP or SBE-FP SHOP issues, and assistance in communicating with CMS;
20. Fulfilling the legal responsibilities related to the efficient functions of QHP Issuers in the FFEs and SBE-FPs, including FF-SHOPs and SBE-FP-SHOPs, as permitted or required by Web-broker's contractual relationships with QHP Issuers; and
21. 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. Web-broker agrees that it will create, collect, disclose, access, maintain, use, or store PII that it receives directly from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employers, and Qualified Employees, and from Hub Web Services, if applicable, only in accordance with all laws as applicable, including section 1411(g) of the PPACA. The Hub Web Services are not available for SHOP.

1. Safeguards. Web-broker 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 the *Non-Exchange Entity System Security and Privacy Plan* (NEE SSP). Furthermore, Web-broker agrees 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. Web-broker will satisfy the requirement in 45 CFR 155.260(b)(2)(v) to bind downstream entities to the same privacy and security standards that apply to Non-Exchange Entities by entering into written agreements

with any downstream entities that will have access to PII as defined in this Agreement. Web-broker must require in writing all downstream and delegated entities to adhere to the terms of this Agreement.

3. Critical Security and Privacy Controls. The critical controls the Web-broker must implement before Web-broker is able to submit any transactions to the FFE production system for individual market enrollments through the FFEs or SBE-FPs and/or assist Qualified Employers and Qualified Employees in purchasing and enrolling in coverage through an FF-SHOP or SBE-FP SHOP:

   a. Email/Web Browser Protections – Including, but not limited to, assurance that transfer protocols are secure and limits the threat of communications being intercepted. NEE SSP SC-7, AU-10, SC-1, SC-4, SC-8, SC-8(1), SC-8(2), SC-13, SC-23, SC-28, and SC-CMS-1 controls.

   b. Malware Protection – Including, but not limited to, protections against known threat vectors within the system's environment to mitigate damage/security breaches. NEE SSP SI-1, SI-2, SI-3, SC-7, SC-1, and SC-CMS-1 controls.

   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. NEE SSP CM-1, CM-2, CM-3, CM-6, CM-8, CM-9, and CM-11 controls.

   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. NEE SSP AU-2, AU-6, RA-3, RA-5, RA-5(1), RA-5(2), CA-7, and SI-5 controls.

   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. NEE SSP AU-6, CM-8, SE-1, and PE-18 controls.

   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. NEE SSP AC-1, AC-2, AC-3, AC-3(9), AC-6, AC-8, AC-14, AC-17, AC-18, AC-19, AC-20, AC-21, IA-1, IA-2, IA-2(1), IA-2(2), IA-2(3), IA-2(8), IA-2(11), IA-3, IA-4, IA-5, IA-5(2), IA-5(3), IA-5(7), IA-5(11), IA-5(15), IA-5(1), IA-6, IA-7, IA-, PE-5, PE-4, PE-3, PS-4, and PS-5 controls.

   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. NEE SSP CM-1, CM-2, CM-3, CM-6, CM-8, CM-9, and CM-11 controls.

   h. Incident Response – Including, but not limited to, the ability to detect security events, investigate, and mitigate or limit the effects of those events. NEE SSP AU-1, AU-2, AU-2(3), AU-3, AU-6, AU-9, AU-10, AU-11, AU-(12), AU-

12(1), IR-1, IR-2, IR-3, IR-3(2), IR-4, IR-4(1), IR-5, IR-6, IR-6(1), IR-7, IR-7(1), IR-8, IR-9, and CP-1 controls.

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. NEE SSP AR-1, AR-4, and AR-3 controls.

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. NEE SSP AR-2 controls.

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. NEE SSP AT-1, AT-2, AT-2(2), and AT-4 controls.

l. Data Retention and Destruction – Including, but not limited to, developing formal policy and procedures for data retention and destruction of PII. NEE SSP AU-11, DM-2, DM-2(1), SI-12, MP-6, and AR-8 controls.

c. PII Received. Subject to the terms and conditions of this Agreement and applicable laws, in performing the tasks contemplated under this Agreement, Web-broker may create, collect, disclose, access, maintain, store, and use the following data and PII from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employers, and Qualified Employees including, but not limited to:

i. For individual market QHP coverage:

- 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

ii. For SHOP QHP coverage:

Category	Description
Employee Personally Identifiable Information	Employee Applicant Name Employee Unique Employer Code Employee Home Address Employee Applicant Mailing Address Employee Applicant Birthdate Employee Social Security Number Employee Applicant Telephone Number (and type) Employee Applicant Email Address Employee Applicant Spoken and Written Language Preference

Category	Description
Employee Personally Identifiable Information (continued)	Employee Tobacco Use Indicator and Last Date of Tobacco Use Employee Sex Employee Race and Ethnicity Employer Business Name If American Indian/Alaska Native: Name and Location of Tribe Health Coverage Type (Individual or Family, if offered) Health Plan Name and ID Number Dental Plan Name and ID Number Other Sources of Coverage Accepting or Waiving Coverage Dependent information, if applicable, including • Dependent Name • Dependent Date of Birth • Dependent Social Security Number • Dependent Relationship to Employee • Dependent Sex • Dependent Spoken and Written Language Preference • Dependent Race and Ethnicity • If American Indian/Alaska Native: Name and Location of Tribe • Dependent Tobacco Use Indicator and Last Date of Tobacco Use • If individual is living outside of home; name of individual, address, phone, e-mail address • Dependent Other Sources of Coverage • Dependent Accepting or Waiving Coverage • Special Circumstances for Employees and Dependents, i.e., marriage, moving, adopting children, losing eligibility for coverage under a group health plan or losing Employer contribution, or giving birth
Employer Offering Coverage Information	Employer Name/"Doing Business As" Employer Federal Tax ID Number Employer Address Business Type Employer Attestation to SHOP Eligibility Requirements Employer Contact Information Employer Contact Name and Title Employer Contact Mailing Address (if different than employer address) Employer Contact Phone Numbers (and type) Employer Contact Spoken and Written Language Preference Employer Contact Email Address Employer Contact Fax Number

Category	Description
Employer Offering Coverage Information (continued)	Secondary Contact Name (optional) Secondary Contact Phone number (and type) Secondary Contact Fax Number Secondary Contact Email Address Secondary Contact Authorizations Employer Coverage Offered Employer-selected AV Levels (Bronze, Silver, Gold, or Platinum) Benchmark Plan Offer of Dependent Coverage Agent/Broker/Assister/Navigator Name, Organization Name, Contact Information, FFM User ID Employer Contribution Information: • Benchmark Plan ID number-Medical Plan • Benchmark Plan ID number-Dental Plan • Percentage towards Employee-Medical Coverage • Percentage towards Employee Dental Coverage • Percentage towards Dependent Medical Coverage • Percentage towards Dependent Dental Coverage • Employer Offering-Single QHP or Single Metal Level or Single Issuer • Employer Offering-Single Stand-alone Dental Plan ("SADP") or multiple SADPs Offer of Stand-alone Dental Coverage Desired Effective Date of Coverage Employee Selection Due Date Waiting Period for New Hires to Enroll Employee List, including • Employee Name • Employee Date of Birth • Employee Age • Employee Social Security Number • Employee Email Address • Employee Employment Status • Employee's Other Coverage • Number of Dependents • Dependent information, including Dependent Name • Dependent Date of Birth • Dependent Age • Dependent Social Security Number • Dependent Email Address • Dependent's Other Coverage

Category	Description
Employer Offering Coverage Information (continued)	Payment Method options, including • Electronic Funds Transfer Information (Checking Account Number, Routing Number) • Credit Card information (Credit Card type, Name on Credit Card, Credit Card Number, Expiration Date, Signature, Signature Date) • Checking Information Employer Attestation to Consolidated Omnibus Budget Reconciliation Act ("COBRA")/Medicare Compliance Questions

d. Collection of PII. PII collected from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees and Qualified Employers—or their legal representatives or Authorized Representatives—in the context of completing an application for QHP, APTC, or CSR eligibility, if applicable, or enrolling in a QHP, or any data transmitted from or through the Hub, if applicable, 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, Enrollee, Qualified Employee, and Qualified Employer.

e. Collection and Use of Information Provided Under Other Authorities. This Agreement does not preclude Web-broker from collecting information from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees and Qualified Employers—or their legal representatives or Authorized Representatives—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. The Hub Web Services are not available for SHOP.

f. Ability of Individuals to Limit Collection and Use. Web-broker agrees to provide the Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee or Qualified Employer the opportunity to opt-in and have Web-broker collect, create, disclose, access, maintain, store and use their PII. Web-broker agrees to provide a mechanism through which the Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee and Qualified Employer can limit Web-broker's creation, collection, disclosure, access, maintenance, storage, and use of their PII to the sole purpose of obtaining Web-broker's assistance in applying for a QHP, APTC or CSR eligibility, if applicable, enrolling in a QHP offered through the FFEs or SBE-FPs (including FF-SHOPs and SBE-FP-SHOPs), and for performing Authorized Functions specified in Section II.a of this Agreement.

g. Incident and Breach Reporting. Web-broker must implement Incident and Breach Handling procedures as required by the SSP and that are consistent with CMS's Incident and Breach notification Procedures. Such policies and procedures must identify the Web-broker's Designated Security and Privacy Official(s), if applicable, and/or identify other personnel authorized to access PII and responsible for reporting to CMS and managing Incidents or Breaches; 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 require reporting of any security and privacy 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 (1) hour after discovery of the Incident or Breach.

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 ("OEP") for the benefit year beginning January 1, 2021.

b. Renewal. This Agreement may be renewed upon the mutual agreement of the Parties for subsequent and consecutive one (1) year periods upon thirty (30) Days' advance written notice to Web-broker.

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 of Agreement with Notice by CMS. The termination of this Agreement and the reconsideration of any such termination shall be governed by the termination and reconsideration standards adopted by the FFEs or SBE-FPs under 45 CFR 155.220. Notwithstanding the foregoing, the Web-broker shall be considered in "Habitual Default" of this Agreement in the event 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 terminate this Agreement upon notice to Web-broker without any further opportunity to resolve the breach and/or non-compliance. CMS may also temporarily suspend the ability of a Web-broker to make its website available to transact information with HHS pursuant to 45 CFR 155.220(c)(4)(ii) or 45 CFR 155.221(d).

c. Termination for Failure to Maintain Valid State Licensure. Web-broker acknowledges and agrees that valid state licensure in each state in which Web-broker will assist consumers in applying for or obtaining coverage under a QHP through an FFE or SBE-FP is a precondition to the Web-broker's authority under this Agreement. Accordingly, CMS may terminate this Agreement upon thirty (30) Days' prior written notice if Web-broker fails to maintain valid licensure in at least one FFE or SBE-FP state, and in each state for which Web-broker facilitates enrollment in a QHP through the FFE or an SBE-FP. Any such termination shall be governed by the termination and reconsideration standards adopted by the FFE under 45 CFR 155.220(g). If Web-broker is a Direct Enrollment Technology Provider, once the contractual relationship with the Agent or Broker who hired or contracted with the Web-broker ends, the entity would no longer meet the applicable definitions under 45 CFR 155.20 to be a Web-broker. Web-broker understands and agrees that in such circumstances CMS may immediately terminate this Agreement for cause.

The Web-broker must provide advance notice to CMS per Section V.a. of this Agreement. If the end of the contractual relationship between the Agent or Broker and Direct Enrollment Technology Provider takes immediate effect, and the Direct Enrollment Technology Provider is unable to provide thirty (30) Days' notice to CMS, the Direct Enrollment Technology Provider must notify CMS within thirty (30) Days after.

d. Destruction of PII. Web-broker covenants and agrees to destroy all PII in its possession at the end of the record retention period required under Appendix A: Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities. If, upon the termination or expiration of this Agreement, Web-broker 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. Web-broker'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. Termination of -registration from the FFEs. Web-broker acknowledges that the termination or expiration of this Agreement will result in the termination of the Web-broker's registration with the FFE .

V. Miscellaneous.

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

- If to CMS, by email at: directenrollment@cms.hhs.gov
- If to Web-broker, to Web-broker's email address on record.

Notices sent by email 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 written notice of such changes in accordance with this provision. Such notice should be provided thirty (30) Days in advance of such change, unless circumstances warrant a shorter timeframe.

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

c. Use of the Hub Web Services. Web-broker will only use a CMS-approved Direct Enrollment pathway when accessing the APIs and web services that facilitate functionality to enroll Consumers through the FFEs and SBE-FPs, which includes compliance with the requirements detailed in Appendix C.

d. Survival. Web-broker's duty to protect and maintain the privacy and security of PII and any other obligation under this Agreement which, by its express terms or nature and context is intended to survive expiration or termination of 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 Web-broker 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 Web-broker. Neither Party is, nor shall either Party hold itself out to be, vested with any power or right to bind the other Party contractually or to act on behalf of the other Party, except to the extent expressly set forth in the PPACA and the regulations codified thereunder, including as codified at 45 CFR part 155.

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. Records. The Web-broker shall maintain all records, whether paper or electronic, that it creates in the normal course of its business in connection with activity under this Agreement for the term of this Agreement and for at least ten (10) Years after the date this Agreement terminates or expires. Subject to applicable legal requirements and reasonable policies, such records shall be made available to CMS to ensure compliance with the terms and conditions of this Agreement. The records shall be made available during regular business hours at the Web-broker offices, and CMS's review shall not interfere unreasonably with the Web-broker business activities.

i. Compliance with Law. Web-broker 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.

j. 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. Web-broker 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*.

k. 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 Web-broker ("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. Web-broker may reject such amendment by providing to CMS, during the CMS notice period, 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.

l. Audit and Compliance Review. Web-broker 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 Web-broker and to audit, inspect, evaluate, examine, and make excerpts, transcripts, and copies of any books, records, documents, and other evidence of Web-broker's compliance with the requirements of this Agreement upon reasonable notice to Web-broker, during Web-broker's regular business hours, and at Web-broker's regular business location. These audit and review rights include the right to audit Web-broker's compliance with and implementation of the privacy and security requirements under this Agreement. Web-broker further agrees to allow reasonable access to the information and facilities, including, but not limited to, Web-broker 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 this Agreement if a Web-broker does not comply with such a compliance review request within seven (7) Business Days. If any of Web-broker's obligations under this Agreement are delegated to other parties, the Web-broker's agreement with any delegated or downstream entities must incorporate this Agreement provision. This clause survives the expiration or termination of this Agreement.

m. APTC Selection and Attestation. Web-broker 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). Web-broker should use the

specific language detailed in the FFE and FF-SHOP Enrollment Manual, available on CMS zONE at https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials, when providing consumers with the ability to attest to an APTC amount.

n. Access to the FFEs and SBE-FPs. Any Web-broker and its assignees or subcontractors—including, employees, developers, agents, representatives, or contractors—cannot remotely connect or transmit data to the FFE, SBE-FP or its testing environments, nor remotely connect or transmit data to a Web-broker's systems that maintain connections to the FFE, SBE-FP or its testing environments, from locations outside of the United States of America or its territories, embassies, or military installations. This includes any such connection through virtual private networks ("VPNs").

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

This "Agreement Between Web-Broker and the Centers for Medicare & Medicaid Services for the Federally-facilitated Exchanges and State-based Exchanges on the Federal Platform" has been signed and executed by:

TO BE FILLED OUT BY WEB-BROKER

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

Plan Year 2020:

_____ _____

Signature of Authorized Official of Web-broker Date

_____

Printed Name and Title of Authorized Official of Web-broker

_____

Web-broker Name

_____

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

_____

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

_____

_____

_____ _____

Web-broker Address Web-broker Contact Number

Web-broker must indicate in the below checkbox whether Web-broker will assist Qualified Employees and/or Qualified Employers in applying for or enrolling in SHOP coverage for PY 2020:

☐ Web-broker ***will*** assist Qualified Employees and/or Qualified Employers in plan year 2020

☐ Web-broker ***will not*** assist Qualified Employees and/or Qualified Employers in plan year 2020

FOR CMS

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

_____ _____

Jeffrey D. Grant **Date**
Deputy Director for Operations
Center for Consumer Information and Insurance Oversight
Centers for Medicare & Medicaid Services

_____ _____

George C. Hoffmann **Date**
Deputy CIO, Acting CISO, and Deputy Director
Office of Information Technology (OIT)
Centers for Medicare & Medicaid Services

Appendix A: Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities

Statement of Applicability

These standards and implementation specifications are established in accordance with Section 1411(g) of the Patient Protection and Affordable Care Act ("PPACA") (42 U.S.C. § 18081(g)), the Federal Information Management Act of 2014 ("FISMA") (44 U.S.C. 3551), 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 the Agreement or 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).

Federally-facilitated Exchanges ("FFEs") will enter into contractual agreements with all Non-Exchange Entities, including Web-brokers that gain access to Personally Identifiable Information ("PII") exchanged with the FFEs (including FF-SHOPs) and State-based Exchanges on the federal platform ("SBE-FPs") (including SBE-FP-SHOPs), or directly from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, or these individuals' legal representatives or Authorized Representatives. This 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 (including FF-SHOPs and SBE-FP-SHOPs). In signing this contractual Agreement, in which this Appendix A has been incorporated, Non-Exchange Entities agree to comply with the security and privacy standards as specified in the *Non-Exchange Entity System Security and Privacy Plan*[2] (NEE SSP) and implementation specifications laid out in this document while performing the Authorized Functions outlined in their respective Agreement(s) with CMS.

NON-EXCHANGE ENTITY PRIVACY AND SECURITY STANDARDS AND IMPLEMENTATION SPECIFICATIONS

Non-Exchange Entities must meet the following privacy and security implementation specifications that are consistent with the Health Insurance Portability and Accountability Act ("HIPAA") of 1996 P.L. 104-191 and the Privacy Act of 1974, 5 U.S.C. § 552a:

(1) *Individual Access to PII. In keeping with the standards and implementation specifications used by the FFEs, a Non-Exchange Entity that maintains and/or stores 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.*

[2] The references in this section to security and privacy controls and implementation standards can be found in the *Non-Exchange Entity System Security and Privacy Plan* located on CMS zONE at the following link: https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials.

a. Standard: Individual Access to PII. A Non-Exchange Entity that maintains and/or stores PII must implement policies and procedures that provide access to PII upon request. The NEE must comply with any additional standards and implementation specifications described in NEE SSP IP-2: Individual Access.

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 its respective Agreement(s) with CMS (including the QHP Issuer Agreement or the Web-broker Agreement).

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

3. Persons legally authorized to act on behalf of Consumers, Applicants, Qualified Individuals, 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 the Subject Individual in determining his or her information or data needs, if such assistance is requested.

5. Subject to paragraphs (1)a.i.6 and 7 below, a Non-Exchange Entity 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 its costs for labor for copying the PII, supplies for creating a paper copy or a copy on electronic media, postage if the PII is mailed, or any costs for preparing an explanation or summary of the PII if the 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. A Non-Exchange Entity 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 FFEs, a Non-Exchange Entity must ensure openness and transparency about policies, procedures, and technologies that directly affect Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers 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. The NEE must comply with any additional standards and implementation specifications described in NEE SSP TR-1: Privacy Notice.

   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 FFEs, the Non-Exchange Entity 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, Qualified Employees, and Qualified Employers —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, FF-SHOP, FF-SBE SHOP, or Non-Exchange Entity obtains informed consent from such individuals. The NEE must comply with any additional standards and implementation specifications described in NEE SSP IP-1: Consent.

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 FFEs, the Non-Exchange Entity must ensure that PII is only created, collected, disclosed, accessed, maintained, stored, and used to the extent necessary to accomplish a specified purpose(s) in the contractual agreement and any appendices. Such*

information shall never be used to discriminate against a Consumer, Applicant, Qualified Individual, or Enrollee.

a. Standard: Creation, Collection, Disclosure, Access, Maintenance, Storage, and Use Limitations. The NEE must comply with the standards and implementation specifications described in NEE SSP AP-1: Authority to Collect. 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. 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); and/or

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

b. Standard: Non-discrimination. Non-Exchange Entity should, 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. 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. 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 his or her SSN is relevant to verification of household income and family size.

      3. Non-Exchange Entity shall not use PII to discriminate, including, but not limited to, employing marketing practices or benefit designs that will have the effect of discouraging the enrollment of individuals with significant health needs in QHPs.

(5) *Data Quality and Integrity. In keeping with the standards and implementation specifications used by the FFEs, Non-Exchange Entity should take reasonable steps to ensure that PII is complete, accurate, and up-to-date to the extent such data are necessary for Non-Exchange Entity's intended use of such data, and that such data have not been altered or destroyed in an unauthorized manner, thereby ensuring the confidentiality, integrity, and availability of PII. The NEE must comply with any additional standards and implementation specifications described in NEE SSP DI-1: Data Quality.*

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

representatives or Authorized Representatives—an opportunity and process 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. The NEE must comply with any additional standards and implementation specifications described in NEE SSP IP-3: Redress and IP-4: Complaint Management.

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. These individuals may also be offered an opportunity to meet with the Responsible Official or his or her 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 his or her 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 his or her delegate) reviews these materials and ultimately does not agree that the PII should be corrected, amended, substituted, or deleted, the requestor shall be informed in writing of the denial, and, if applicable, the availability of any appeal procedures. If available, the notification must identify the appropriate appeal authority including that authority's name, title, and contact information.

b. Standard: Verification of Identity for Requests to Amend, Correct, Substitute, or Delete PII. In keeping with the standards and implementation specifications used by the FFEs, a Non-Exchange Entity that maintains and/or stores 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 Non-Exchange Entity. This includes confirmation of an individual's 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 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 members of 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 Non-Exchange Entity, a Non-Exchange Entity that maintains and/or stores PII shall maintain an accounting of any and all disclosures. The NEE must comply with any additional standards and implementation specifications described in NEE SSP AR-8: Accounting of 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, Enrollees, Qualified Employees, and 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 FFEs, a Non-Exchange Entity 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. The NEE must comply with any additional standards and implementation specifications described in NEE SSP SE-2 Privacy Incident Response.*

a. Standard: Reporting. The Non-Exchange Entity must implement Incident and Breach Handling Procedures that are consistent with CMS' Incident and Breach

Notification Procedures[3] 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 Security and Privacy Official(s), 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, if applicable, for containment purposes; and

3. Require reporting of any security and privacy 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. The NEE must comply with any additional standards and implementation specifications described in NEE SSP AR-1: Governance and Privacy Program.

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

[3] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-08-Incident-Response.pdf

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. Penetration testing;

c. Adherence to privacy program policies;

d. Network and component vulnerability scanning;

e. Configuration assessment;

f. Documentation review;

g. Personnel interviews; and

h. 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. NEE SSP SC-7, AU-10, SC-1, SC-4, SC-8, SC-8(1), SC-8(2), SC-13, SC-23, SC-28, and SC-CMS-1 controls.

b. Malware Protection – Including, but not limited to, protections against known threat vectors within the system's environment to mitigate damage/security breaches. NEE SSP SI-1, SI-2, SI-3, SC-7, SC-1, and SC-CMS-1 controls.

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. NEE SSP CM-1, CM-2, CM-3, CM-6, CM-8, CM-9, and CM-11 controls.

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. NEE SSP AU-2, AU-6, RA-3, RA-5, RA-5(1), RA-5(2), CA-7, and SI-5 controls.

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. NEE SSP AU-6, CM-8, SE-1, and PE-18 controls.

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. NEE SSP AC-1, AC-2, AC-3, AC-3(9), AC-6, AC-8, AC-14, AC-17, AC-18, AC-19, AC-20, AC-21, IA-1, IA-2, IA-2(1), IA-2(2), IA-2(3), IA-2(8), IA-2(11), IA-3, IA-4, IA-5, IA-5(2), IA-5(3), IA-5(7), IA-5(11), IA-5(15), IA-5(1), IA-6, IA-7, IA-, PE-5, PE-4, PE-3, PS-4, and PS-5 controls.

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. NEE SSP CM-1, CM-2, CM-3, CM-6, CM-8, CM-9, and CM-11 controls.

h. Incident Response – Including, but not limited to, the ability to detect security events, investigate, and mitigate or limit the effects of those events. NEE SSP AU-1, AU-2, AU-2(3), AU-3, AU-6, AU-9, AU-10, AU-11, AU-(12), AU-12(1), IR-1, IR-2, IR-3, IR-3(2), IR-4, IR-4(1), IR-5, IR-6, IR-6(1), IR-7, IR-7(1), IR-8, IR-9, and CP-1 controls.

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. NEE SSP AR-1, AR-3, and AR-4 controls.

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. NEE SSP AR-2 control.

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. NEE SSP AT-1, AT-2, AT-2(2), and AT-4 controls.

l. Data Retention and Destruction – Including, but not limited to, developing formal policy and procedures for data retention and destruction of PII. NEE SSP AU-11, DM-2, DM-2(1), SI-12, MP-6, AR-8 controls.

(6) Non-Exchange Entity System Security Plan ("SSP") which is based on the National Institute for Standards and Technology Special Publication 800-53, Revision 4. Independent third-party auditor verification and documentation of the Non-Exchange Entity's compliance with some or all of NEE SSP controls 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: Annual Security and Privacy Attestation Report 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 by July 1, 2020.

(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 or Appendices that is not defined therein or in this Appendix has the meaning provided in 45 CFR 155.20.

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

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

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

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

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

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

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

(8) **Breach** has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017), and means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: (1) a person other than an authorized user accesses or potentially accesses Personally Identifiable Information or (2) an authorized user accesses or potentially accesses Personally Identifiable Information ("PII") for anything other than an authorized purpose.

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

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

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

(12) **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.

(13) **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. The Hub is not available for SHOP.

(14) **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 ("FFE") website, including the collection of personal and financial information necessary for Consumer, Applicant, Qualified Individual, or Enrollee account creations; Qualified Health Plan ("QHP") application submissions; and Insurance

Affordability Program eligibility determinations. The Hub Web Services are not available for SHOP.

(15) **Consumer** means a person who, for himself or herself, or on behalf of another individual, seeks information related to eligibility or coverage through a QHP or Insurance Affordability Program, or whom an Agent, Broker, or Web-broker registered with the FFE, Navigator, Issuer, Certified Application Counselor, or other entity assists in applying for a QHP, applying for APTC and CSRs, and/or completing enrollment in a QHP through the FFEs or State-based Exchanges on the federal platform ("SBE-FPs") for individual market coverage.

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

(17) **Customer Service** means assistance regarding eligibility and Health Insurance Coverage provided to a Consumer, Applicant, or Qualified Individual, including, but not limited to, responding to questions and complaints; providing information about eligibility; applying for APTC and CSRs, and Health Insurance Coverage; and explaining enrollment processes in connection with the FFEs. Includes assistance provided to Qualified Employers and Qualified Employees regarding FF-SHOP and SBE-FP SHOP coverage.

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

(19) **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 Privacy Notice statement, responsible for the development and implementation of the privacy policies and procedures of the Non-Exchange Entity, and ensuring the Non-Exchange Entity has in place appropriate safeguards to protect the privacy of PII.

(20) **Direct Enrollment** means the process by which a Web-broker or QHP Issuer may enroll an Applicant in a QHP in a manner that is considered through the Exchange consistent with 45 C.F.R. 155.220(c), 155.221, 156.265, and 156.1230.

(21) **Direct Enrollment ("DE") Entity** has the meaning set forth in 45 CFR 155.20.

(22) **Direct Enrollment ("DE") Pathway** means the APIs and functionality comprising the systems that enable DE as provided, owned, and maintained by CMS.

(23) **Direct Enrollment Technology Provider** has the meaning set forth in 45 CFR 155.20.

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

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

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

(27) **Federally-facilitated Exchange ("FFE")** means an **Exchange** (or **Marketplace**) established by the Department of Health and Human Services (HHS) and operated by CMS under Section 1321(c)(1) of the PPACA for individual or small group market coverage, including the Federally-facilitated Small Business Health Options Program (**FF-SHOP**). **Federally-facilitated Marketplaces (FFMs)** has the same meaning as FFEs.

(28) **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).

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

(30) **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).

(31) **HHS** means the United States Department of Health & Human Services.

(32) **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.

(33) **Incident**, or **Security Incident**, has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017) and means an occurrence that: (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

(34) **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.

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

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

(2) A State Children's Health Insurance Program ("CHIP") under title XXI of the Social Security Act.

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

(4) A program that makes coverage in a QHP 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 CSRs established under section 1402 of the PPACA.

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

(37) **Non-Exchange Entity** has the meaning at 45 CFR 155.260(b)(1), and includes, but not limited, to QHP Issuers, Navigators, Agents, Brokers, and Web-brokers.

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

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

(40) **Personally Identifiable Information ("PII")** has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017), and refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

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

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

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

(46) **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.

(47) **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.

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

(49) **State-based Exchange ("SBE")** means an Exchange established by a State that receives approval to operate under 45 C.F.R. § 155.105. **State-based Marketplace ("SBM")** has the same meaning as SBE.

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

(51) **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.

(52) **Subject Individual** means that individual to whom a System of Records Notice (SORN) Record pertains.

(53) **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.

(54) **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.

(55) **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.

(56) **Web-broker** has the meaning set forth in 45 CFR 155.20.

(57) **Workforce** means a Non-Exchange Entity's, FFE's, or SBE-FP's employees, Agents, contractors, subcontractors, officers, directors, 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

The Hub and Hub Web Services are not available for the Small Business Health Options Program (SHOP). Therefore, this Appendix is not applicable for Web-broker participation in SHOP.

(1) Web-broker must possess a unique Partner ID assigned by the Centers for Medicare & Medicare Services ("CMS"). Web-broker must use its unique Partner ID when interacting with the CMS Data Services Hub ("Hub") and the Direct Enrollment ("DE") Application Program Interfaces ("APIs") for Web-broker's own line of business.

If the Web-broker provides a DE pathway to an Issuer for the exclusive use of enrollment in that Issuer's plans, the Web-broker must ensure that each Issuer maintains its own, unique Partner ID with the Hub.

(2) Web-broker must complete testing for each Hub-related transaction it will implement, and it 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 Health Insurance Portability and Accountability Act ("HIPAA") of 1996 compliance standards, or other CMS-approved standards, and to process electronic data and information transmitted by Web-broker to the Hub. The capability to submit these test transactions will be maintained by Web-broker throughout the term of this Agreement.

(3) 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.

(4) Web-broker 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 Federally-facilitated Exchange ("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 https://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.

(5) Web-broker 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.[4]

[4] 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 Web-broker so that Web-broker may discern the activity related to enrollment functions of persons they serve. Web-broker may also use the transported data to receive descriptions of financial transactions from CMS.

(6) Web-broker 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 (2) above.

(7) If Web-broker 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 Web-broker as being in the proper format and compatible with the FFE system. Entities that enter into contract with Web-broker and access Personally Identifiable Information ("PII") are required to maintain the same or more stringent security and privacy controls as Web-broker.

(8) Web-broker must successfully complete an Operational Readiness Review to the satisfaction of CMS before Web-broker is able to submit any transactions to the FFE production system or agrees that CMS may require further reviews or corrective actions at any time during the term of this Agreement. The Operational Readiness Review will assess Web-broker'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. Web-broker 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

Annual Security and Privacy Attestation Report – *Web-broker*

Self-Attestation for Year: (e.g. January 2019 – December 2019)
Date Completed:

Attestation Identification	
Web-broker	
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. NEE SSP SC-7, AU-10, SC-1, SC-4, SC-8, SC-8(1), SC-8(2), SC-13, SC-23, SC-28, and SC-CMS-1 controls.				
2. Malware Protection: Including, but not limited to, protections against known threat vectors within the system's environment to mitigate damage/security breaches. NEE SSP SI-1, SI-2, SI-3, SC-7, SC-1, and SC-CMS-1 controls.				
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. NEE SSP CM-1, CM-2, CM-3, CM-6, CM-8, CM-9, and CM-11 controls.				
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. NEE SSP AU-2, AU-6, RA-3, RA-5, RA-5(1), RA-5(2), CA-7, and SI-5 controls.				

Critical Control	Met	Not Met	N/A	Date (Day/Month/Year)
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. NEE SSP AU-6, CM-8, SE-1, and PE-18 controls.				
6. 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. NEE SSP AC-1, AC-2, AC-3, AC-3(9), AC-6, AC-8, AC-14, AC-17, AC-18, AC-19, AC-20, AC-21, IA-1, IA-2, IA-2(1), IA-2(2), IA-2(3), IA-2(8), IA-2(11), IA-3, IA-4, IA-5, IA-5(2), IA-5(3), IA-5(7), IA-5(11), IA-5(15), IA-5(1), IA-6, IA-7, IA-, PE-5, PE-4, PE-3, PS-4, and PS-5 controls.				
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. NEE SSP CM-1, CM-2, CM-3, CM-6, CM-8, CM-9, and CM-11 controls.				
8. Incident Response: Including, but not limited to, the ability to detect security events, investigate, and mitigate or limit the effects of those events. NEE SSP AU-1, AU-2, AU-2(3), AU-3, AU-6, AU-9, AU-10, AU-11, AU-(12), AU-12(1), IR-1, IR-2, IR-3, IR-3(2), IR-4, IR-4(1), IR-5, IR-6, IR-6(1), IR-7, IR-7(1), IR-8, IR-9, and CP-1 controls.				
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. NEE SSP AR-1, AR-4, and AR-3 controls.				
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. NEE SSP AR-2 controls.				

Critical Control	Met	Not Met	N/A	Date (Day/Month/Year)
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. NEE SSP AT-1, AT-2, AT-2(2), and AT-4 controls.				
12. Data Retention and Destruction: Including, but not limited to, developing formal policy and procedures for data retention and destruction of PII. NEE SSP AU-11, DM-2, DM-2(1), SI-12, MP-6, and AR-8 controls.				

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

Self- Attestation for Year: [ ]
(e.g., January 2019 – December 2019)
Date Completed:

System Security Officer

Signature Date

Privacy Officer

Signature Date

Business Owner

Signature Date