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 that uses a non-FFE Internet website in accordance with 45 C.F.R. §§ 155.220(c) 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 are 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 Affordable Care Act ("ACA") 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, Qualified Employers, and Qualified Employees 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 C.F.R. § 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 ACA 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 an Agent or Broker 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 Employees, and Qualified Employers—or these individuals' legal representatives or Authorized Representatives—to perform the Authorized Functions described in Section II.a of this Agreement. The Hub Web Services are not available for SHOP.

6. 45 C.F.R. § 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 standards in 45 C.F.R. §§ 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 C.F.R. § 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 for , Appendix B: Annual Security and Privacy Assessment (SPA), 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 C: Definitions. Any capitalized term that is not defined herein or in Appendix C: Definitions has the meaning provided in 45 C.F.R. § 155.20.

II. Acceptance of Standard Rules of Conduct.

Web-broker and CMS are entering into this Agreement to satisfy the requirements under 45 C.F.R. § 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 the Appendices, which are incorporated by reference in this Agreement, while and as engaging in any activity as Web-broker for purposes of the ACA. Web-broker shall strictly adhere to the privacy and security standards—and ensure that its employees, officers, directors, contractors, subcontractors, agents, and

[1] The references in this Agreement to security and privacy controls and implementation standards can be found in the NEE SSP located on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit.

representatives strictly 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 the 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, Qualified Employers, and Qualified Employees—or these individuals' legal representatives or Authorized Representatives—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, Qualified Employers and Qualified Employees—or these individuals' legal representatives or Authorized Representatives—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 for Handling 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, Qualified Employees—or these individuals' legal representatives or Authorized Representatives—and from Hub Web Services, if applicable, only in accordance with all laws as applicable, including section 1411(g) of the ACA. The Hub Web Services are not available for SHOP.

    1. Security and Privacy Controls. Web-broker agrees to monitor, periodically assess, and update its security and privacy controls documented in the NEE SSP and related system risks to ensure the continued effectiveness of those controls in accordance with this Agreement, including Appendix A: Privacy and Security Standards for , Appendix B: Annual Security and Privacy Assessment (SPA), NEE Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide, and the NEE SSP. Furthermore, Web-broker agrees to timely inform the Exchange of any material change in its administrative, technical, or operational environments, or any material change that would require an alteration of the privacy and security standards within this Agreement.

2. Downstream and Delegated Entities. Web-broker will satisfy the requirement in 45 C.F.R. § 155.260(b)(2)(v) to bind downstream and delegated entities to the same privacy and security standards that apply to Non-Exchange Entities by entering into written agreements with any downstream and delegated entities that will have access to PII as defined in this Agreement. Web-broker must require in writing all downstream and delegated entities adhere to the terms of this Agreement.

c. Collection of PII. 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 CMS, Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employers, and Qualified Employees—or these individuals' legal representatives or Authorized Representatives—including, but not limited to:

1. 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 CHIP eligibility indicator, start and end dates
- Applicant QHP eligibility indicator, start and end dates
- Applicant APTC percentage and amount applied eligibility indicator, start and end dates
- Applicant household income
- Applicant maximum APTC amount
- Applicant CSR eligibility indicator, start and end dates
- Applicant CSR level
- Applicant QHP eligibility status change
- Applicant APTC eligibility status change
- Applicant CSR eligibility status change
- Applicant Initial or Annual Open Enrollment Indicator, start and end dates
- Applicant Special Enrollment Period eligibility indicator and reason code
- Contact name
- Contact address
- Contact birthdate
- Contact telephone number
- Contact email
- Contact spoken and written language preference
- Enrollment group history (past six months)
- Enrollment type period
- FFE Applicant ID

- FFE Member ID
- Issuer Member ID
- Net premium amount
- Premium amount, start and end dates
- Credit or Debit Card Number, name on card
- Checking account and routing number
- Special Enrollment Period reason
- Subscriber indicator and relationship to subscriber
- Tobacco use indicator and last date of tobacco use
- Custodial parent
- Health coverage
- American Indian/Alaska Native status and name of tribe
- Marital status
- Race/ethnicity
- Requesting financial assistance
- Responsible person
- Dependent name
- Applicant/dependent sex
- Student status
- Subscriber indicator and relationship to subscriber
- Total individual responsibility amount

2. For SHOP QHP coverage:

Category	**Description**
	Employee PII
	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
	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

Category Description	
	Other Sources of Coverage
	Accepting or Waiving Coverage
Employee PII continued	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, email 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
	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

Category	Description
Employer Offering Coverage Information continued	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 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. Use of PII. PII collected from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals' 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—or these individuals' legal representatives or Authorized Representatives.

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 these individuals' 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. Commitment to Protect PII. Web-broker shall not release, publish, or disclose Consumer, Applicant, Qualified Individual, or Enrollee PII to unauthorized personnel, and shall protect such Information in accordance with provisions of any laws and regulations governing the adequate safeguarding of Consumer, Applicant, Qualified Individual, or Enrollee PII, the misuse of which carries with it the potential to cause financial, reputational and other types of harm.

   1. Technical leads must be designated to facilitate direct contacts between the Parties to support the management and operation of the interconnection.

   2. The overall sensitivity level of data or Information that will be made available or exchanged across the interconnection will be designated as MODERATE as determined by Federal Information Processing Standards (FIPS) Publication 199.

   3. Web-broker agrees to comply with all federal laws and regulations regarding the handling of PII—regardless of where the organization is located or where the data are stored and accessed.

   4. Web-broker's Rules of Behavior must be at least as stringent as the HHS Rules of Behavior. [2]

   5. Web-broker understands and agrees that all financial and legal liabilities arising from inappropriate disclosure or Breach of Consumer, Applicant, Qualified Individual, or Enrollee PII while such Information is in the possession of Web-broker shall be borne exclusively by Web-broker.

   6. Web-broker shall train and monitor staff on the requirements related to the authorized use and sharing of PII with third parties and the consequences of

[2] The HHS Rules of Behavior are available at the following link: https://www.hhs.gov/ocio/policy/hhs-rob.html.

unauthorized use or sharing of PII, and periodically audit their actual use and disclosure of PII.

g. Ability of Individuals to Limit Collection and Use of PII. Web-broker agrees to provide the Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee or Qualified Employer—or these individuals' legal representatives or Authorized Representatives—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—or these individuals' legal representatives or Authorized Representatives—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 performing Authorized Functions specified in Section II.a of this Agreement.

h. Incident and Breach Reporting. Web-broker must implement Incident and Breach Handling procedures as required by the NEE 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. Web-broker agrees to report any 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 24 hours from knowledge of the Breach. Incidents must be reported to the CMS IT Service Desk by the same means as Breaches within 72 hours from knowledge of the Incident.

III. Approval and Renewal Minimum Direct Enrollment ("DE") Program Participation Requirements.

a. Completion of Operational Readiness Review Required Under 45 C.F.R. §§ 155.220(c)(6), 155.221(b)(4), and 155.221(f).

1. End-to-End Testing and Enrollment Validation Requirement. In order to be approved as a Web-broker, or to maintain status as an Existing Web-broker during Web-broker Agreement renewal, Web-broker must demonstrate a successful end-to-end DE transaction through any of the following: a history of enrollments completed via Classic DE or EDE during the term of the prior year's Web-broker Agreement or by end-to-end testing either with the Hub or during the EDE business audit submission process within the term of the prior year's Web-broker Agreement, as applicable.

2. Operational and Oversight Information Form. In order to be approved as a Web-broker, Web-broker must submit an Operational and Oversight Information Form to CMS in the form and manner specified by CMS. In order to maintain status as an Existing Web-broker during Web-broker Agreement renewal, Web-broker must submit annually an Operational and Oversight Information Form to CMS in the form and manner specified by CMS.

3. Operational Information. When onboarding annually during Agreement renewal, and upon request, the Web-broker must provide CMS operational Information, including, but not limited to, its Designated Representative's National Producer Number (NPN), State licensure Information, and Information about its downstream Agents/Brokers, if applicable.

4. Pre-Approval Website Review. Prospective Web-brokers must receive and resolve any designated compliance findings identified by CMS during a pre-approval website review prior to receiving a countersigned Web-broker Agreement. To facilitate this review, upon request, a Prospective Web-broker must provide CMS with a set of credentials CMS can use to access the Prospective Web-broker's testing DE Environment (i.e., the pre-production environment) to complete the website review of the Prospective Web-broker's DE Environment. The Prospective Web-broker must ensure that the testing credentials are valid and that all APIs and components in the testing DE Environment are accessible for the duration of the review. This provision does not apply to Existing Web-brokers that have received a CMS website review during the term of the prior year's Web-broker Agreement.

5. Designated Representative Registration and Training with the Exchange. Web-broker's Designated Representative(s) must complete the applicable annual registration and training requirements with the Exchange. Web-broker, including Agent or Broker Direct Enrollment Technology Provider, must provide this information to CMS to connect to the DE or EDE web services in production.

6. Privacy and Security Documentation. In order to receive approval to participate in DE and utilize an approved DE Environment, Web-brokers must submit the complete set of documents outlined in Table 1 of Appendix A: Privacy and Security Standards for Web-brokers to CMS, except as noted in the "Submission Requirements" column and must comply with the privacy and security audit requirements under Section IX of this Agreement. The annual assessment results that serve as the basis for the documentation in Table 1 of Appendix B: Annual Security and Privacy Assessment (SPA) are only valid for a period of 365 Days from the completion date of the assessment. Web-brokers must complete the continuous monitoring requirements detailed in the Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide.[3]

   The Web-broker must conduct penetration testing which examines the network, application, device, and physical security of its DE Environment to discover weaknesses and identify areas where the security posture needs improvement, and subsequently, ways to remediate the discovered vulnerabilities. Web-brokers must adhere to the requirements for Penetration Testing described in Section V.b and Appendix B: Annual Security and Privacy Assessment (SPA) of this Agreement.

b. Web-broker Public List Requirements. In order to be listed on CMS's Web-broker Public List, Web-brokers must have completed the applicable onboarding or renewal processes (see Section III.a of this Agreement); have a valid, countersigned Web-broker

[3] The ISCM Strategy Guide is available on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit.

Agreement; and have an active, approved Secure Sockets Layer (SSL) production certificate with the Hub for the applicable plan year or an SSL production certificate pending CMS approval under Section III.a.5 of this Agreement.

IV. Downstream Use of Web-broker's DE Environment.

a. Downstream Agent/Broker and DE Entity Application Assister Use of a Web-broker's DE Environment. A Web-broker that provides access to its DE Environment to downstream Agents and Brokers and DE Entity Application Assisters, consistent with 45 C.F.R. §§ 155.220(c)(4) and 155.221(c), must provide a DE Environment to its downstream Agents and Brokers and DE Entity Application Assisters that complies with this Agreement and the Web-broker requirements in 45 C.F.R. §§ 155.220 and 155.221. Web-broker must not provide the capability for downstream Agents/Brokers to use its DE Environment through the third party's own website or otherwise outside of Web-broker's approved website. The use of embedding tools and programming techniques by downstream Agents/Brokers, such as iframe technical implementations, that may enable the distortion, manipulation, or modification of the approved DE Environment and the overall DE End-User experience developed by Web-broker are prohibited.

As part of the DE or EDE-facilitated application and QHP application processes, Web-broker must not enable or allow the selection of QHPs by a consumer or Agent/Broker on a third-party website that exists outside of the Web-broker's approved DE Environment. This includes pre-populating or pre-selecting a QHP for a consumer that was selected on a downstream Agent's/Broker's website or a lead generator's website. This prohibition does not extend to websites that are provided, owned, and maintained by entities subject to CMS regulations for QHP display (i.e., Web-brokers and QHP Issuers).

The Web-broker must have a written contract or other written arrangement with the downstream Agent or Broker or DE Entity Application Assisters that governs the arrangement and requires the adherence to the terms of this Agreement.

Upon request, Web-broker must provide CMS with information about its downstream Agents/Brokers, Web-broker's oversight of its downstream Agents/Brokers, and the DE Environment(s) it provides to each of its downstream Agents/Brokers.

b. QHP Issuer Use of a Web-broker's DE Environment. Web-broker may provide access to its DE Environment to QHP Issuers for use by the QHP Issuer and/or the QHP Issuer's downstream Agents and Brokers and DE Entity Application Assisters that is branded and specific to that QHP Issuer. In these cases, the Web-broker would be considered a downstream and delegated entity of the QHP Issuer under 45 C.F.R. § 156.340. There must be a written contract or other written arrangement between the Web-broker and the QHP Issuer that governs the arrangement and requires adherence to the terms of this Agreement. The QHP Issuer's DE Environment that is provided by the Web-broker must comply with the DE requirements applicable to QHP Issuers in 45 C.F.R. §§ 155.221 and 156.1230.

V. DE Environment and Website Requirements.

a. Maintenance of an Accurate Testing DE Environment. Web-broker must maintain a testing DE Environment that accurately represents the Web-broker's production DE Environment and integration with the Classic DE pathway, including functional use of all

DE APIs. Web-brokers must maintain at least one testing DE Environment that reflects the Web-broker's current production DE Environments when developing and testing any prospective changes to its production DE Environments. This will require Web-broker to develop one or more separate testing DE Environments (other than production and the testing DE Environment that reflects production) for developing and testing prospective changes to Web-broker's production DE Environments. Network traffic into and out of all non-production environments is only permitted to facilitate system testing and must be restricted by source and destination access control lists, as well as ports and protocols, as documented in the NEE SSP, SA-11 implementation standard. Web-broker must not submit actual PII to the FFE Testing Environments. The Web-broker shall not submit test data to the FFE Production Environments. Web-broker's testing DE Environment shall be readily accessible to applicable CMS staff and contractors via the Internet to complete CMS audits.

Upon request, Web-broker must provide CMS with a set of credentials and any additional instructions necessary so that CMS can access the testing DE Environment that reflects the Web-broker's production environment to complete audits or otherwise confirm compliance of Web-broker's production DE Environments. The Web-broker must be able to provide test credentials for all DE Environments that Web-broker hosts or provides (and/or prototypes of those DE Environments), including, but not limited to, the Web-broker's Consumer-facing DE Environment, Web-broker's Agent/Broker-facing DE Environment, a Consumer-facing website that the Web-broker provides for use by Agents or Brokers, and an Agent- or Broker-facing DE Environment that the Web-broker provides for use by Agents/Brokers. Web-broker must ensure that the testing credentials are valid and that all APIs and components in the testing DE Environment, including the remote identity proofing (RIDP) services, are readily accessible via Internet for CMS to audit or otherwise confirm compliance of Web-broker's production DE Environment as determined necessary by CMS.

b. Penetration Testing. The DE Entity must conduct penetration testing which examines the network, application, device, and physical security of its DE Environment to discover weaknesses and identify areas where the security posture needs improvement, and subsequently, ways to remediate the discovered vulnerabilities. Before conducting the penetration testing, the DE Entity must execute a Rules of Engagement with its Auditor's penetration testing team. The DE Entity must also notify its CMS designated technical counterparts on its annual penetration testing schedule a minimum of 5 business days prior to initiation of the penetration testing using the CMS-provided form.[4] During the penetration testing, the Auditor's testing team shall not target IP addresses used for the CMS and Non-CMS Organization connection and shall not conduct penetration testing in the production environment. The penetration testing shall be conducted in the lower environment that reflects the DE Entity's current production environment.

c. Limit Concurrent Sessions. The Web-broker must limit the number of concurrent sessions to one (1) session per a single set of credentials/FFE user ID. However, multiple sessions associated with a single set of credentials/FFE user ID that is traceable to a

[4] The Penetration Testing Notification Form is available at the following links: https://zone.cms.gov/document/privacy-and-security-audit.

single device/browser is permitted.

d. Health Reimbursement Arrangement (HRA) Messaging. If Web-broker implements full HRA functionality, Web-broker must implement required User Interface (UI) messaging for qualified individuals who have an HRA offer that is tailored to the type and affordability of the HRA offered to the qualified individuals consistent with CMS guidance. Required UI messaging for various scenarios is detailed in the FFEs DE API for Web-brokers/Issuers Technical Specifications document.[5]

e. APTC Selection and Attestation. Web-broker must allow Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—to select and attest to an APTC amount, if applicable, in accordance with 45 C.F.R. § 155.310(d)(2). Web-broker should use the specific language detailed in the FFE and FF-SHOP Enrollment Manual[6] when providing Consumers, Applicants, Qualified Individuals, and Enrollees—or these individuals' legal representatives or Authorized Representatives—with the ability to attest to an APTC amount.

VI. 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") under 45 C.F.R. § 155.410(e)(3) for the benefit year beginning January 1, 2025.

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.

VII. Suspension.

a. Suspension Pursuant to 45 C.F.R. §§ 155.220 and 155.221. The suspension of the ability of Web-broker to transact information with the Exchange shall be governed by the suspension standards adopted by the FFEs or SBE-FPs under 45 C.F.R. §§ 155.220 and 155.221.

b. Duration of Suspension. Consistent with the standards under 45 C.F.R. §§ 155.220 and 155.221, Web-broker will remain suspended until Web-broker remedies or sufficiently mitigates the issue(s) that were the basis for the suspension to HHS's satisfaction. If this Agreement expires prior to HHS removing the suspension, HHS will not execute a subsequent Web-broker Agreement with Web-broker until Web-broker remedies or sufficiently mitigates the issue(s) to HHS's satisfaction.

VIII. 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.

[5] The document Direct Enrollment API Specs is available on CMS zONE at the following link: https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials.
[6] The SHOP Enrollment Manual is available on CMS zONE at the following link: https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials.

Web-broker must reference and complete the NEE Decommissioning Plan and NEE Decommissioning Close Out Letter in situations where Web-broker will retire or decommission its DE Environment.[7]

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 C.F.R. § 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 C.F.R. § 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 C.F.R. §§ 155.220(c)(4)(ii) or 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 assists Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals' legal representatives or Authorized Representatives—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 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 standards adopted by the FFE under 45 C.F.R. § 155.220(g) and (h). If Web-broker is an Agent or Broker Direct Enrollment Technology Provider and maintains no contractual relationships with Agents or Brokers and is not owned or operated by an Agent or Broker, the entity would no longer meet the applicable definition under 45 C.F.R. § 155.20 to be an Agent or Broker Direct Enrollment Technology Provider. Web-broker understands and agrees that in such circumstances CMS may immediately terminate this Agreement for cause, or the Agent or Broker Direct Enrollment Technology Provider may provide advance notice to CMS to terminate this agreement without cause per Section VIII.a of this Agreement. If the Agent or Broker Direct Enrollment Technology Provider is unable to provide thirty (30) Days' advance notice to CMS, the Agent or Broker Direct Enrollment Technology Provider must notify CMS within thirty (30) Days after the entity no longer meets the applicable definition under 45 C.F.R. § 155.20 to be an Agent or Broker Direct Enrollment Technology Provider.

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 the NEE SSP, which is consistent with NIST SP 800-88 Rev. 1. If, upon the termination or expiration of this Agreement, Web-broker has in its possession PII for which no retention period is specified in the NEE SSP, such PII shall be destroyed within thirty (30) Days of the termination or

[7] The Non-Exchange Entity (NEE) Decommissioning Plan and NEE Decommissioning Close Out Letter are available on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit

expiration of this Agreement. Web-broker's duty to protect and maintain the privacy and security of PII, as provided for in the NEE SSP, 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.

IX. Privacy and Security Audit Requirement. In order to receive approval to participate in DE and utilize an approved DE Environment, Web-broker must contract with one or more independent Auditor(s) consistent with this Agreement's provisions and applicable regulatory requirements to conduct an annual security and privacy assessment (SPA) as described in Appendix B: Annual Security and Privacy Assessment (SPA), the ISCM Strategy Guide, and the NEE SSP.

The Auditor must document and attest in the SPA documentation that Web-broker's DE Environment, including its website and operations, complies with the terms of this Agreement, other applicable agreement(s) with CMS (including the EDE Business Agreement and Interconnection Security Agreement), the Framework for the Independent Assessment of Security and Privacy Controls, and applicable program requirements. EDE Entity must submit the resulting SPA documentation to CMS. The SPA must detail EDE Entity's compliance with the requirements set forth in Appendix B, including any requirements set forth in CMS guidance referenced in Appendix B The SPA that Web-broker submits to CMS must demonstrate that Web-broker's Auditor(s) conducted its review in accordance with the review standards set forth in Appendix B, the ISCM Strategy Guide, and the NEE SSP.

CMS will approve Web-broker's DE Environment only once it has reviewed and approved the privacy and security audit findings reports. Final approval of Web-broker's DE Environment will be evidenced by CMS countersigning the ISA with Web-broker. Upon receipt of the counter-signed ISA, Web-broker will be approved to use its approved DE Environment consistent with applicable regulations, this Agreement, and the ISA.

a. Identification of Auditor(s) and Subcontractors of Auditor(s). All Auditor(s), including any Auditor(s) that has subcontracted with Web-broker's Auditor(s), will be considered Downstream or Delegated Entities of Web-broker pursuant to Web-broker's respective agreement(s) with CMS and applicable program requirements. Web-broker must identify each Auditor it selects, and any subcontractor(s) of the Auditor(s), in Appendix E: Auditor Identification of this Agreement. Web-broker must also submit a copy of the signed agreement or contract between the Auditor(s) and Web-broker to CMS.

b. Conflict of Interest. For any arrangement between Web-broker and an Auditor for audit purposes covered by this Agreement, Web-broker must select an Auditor that is free from any real or perceived conflict(s) of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence. Web-broker must disclose to HHS any financial relationships between the Auditor, and individuals who own or are employed by the Auditor, and individuals who own or are employed by a Web-broker for which the Auditor is conducting an ORR privacy and security audit pursuant to 45 C.F.R. §§ 155.220(c)(6)(iv), 155.221(b)(4)(ii),

and 155.221(f). Web-broker must document and disclose any conflict(s) of interest in the form in Appendix F: Conflict of Interest Disclosure Form, if applicable.

c. Auditor Independence and Objectivity. Web-broker's Auditor(s) must remain independent and objective throughout the audit process. An Auditor is independent if there is no perceived or actual conflict of interest involving the developmental, operational, and/or management chain associated with the DE Environment and the determination of security and privacy control effectiveness. Web-broker must not take any actions that impair the independence and objectivity of Web-broker's Auditor. Web-broker's Auditor must attest to their independence and objectivity in completing the DE audit(s).

d. Required Documentation. Web-broker must maintain and/or submit the required documentation detailed in Appendix B: Annual Security and Privacy Assessment (SPA), including templates provided by CMS, to CMS in the manner specified in Appendix B: Annual Security and Privacy Assessment (SPA). Documentation that Web-broker must submit to CMS (as set forth in Section III and Appendices B, E, and F of this Agreement) will constitute Web-broker's Application.

X. 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; 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. Except as otherwise provided in this Section, Web-broker shall not assign this Agreement in whole or in part, whether by merger, acquisition, consolidation, reorganization, or otherwise any portion of the services to be provided by Web-broker under this Agreement without the express, prior written consent of CMS, which consent may be withheld, conditioned, granted, or denied in CMS' sole discretion. Web-broker must provide written notice at least thirty (30) Days prior to any such proposed assignment, including any change in ownership of Web-broker or any change in management or ownership of the DE Environment. Notwithstanding the foregoing, CMS does not require prior written consent for subcontracting arrangements that do not involve the operation, management, or control of the DE Environment. Web-broker must report all subcontracting arrangements on its annual Operational and Oversight Information form during the annual Web-broker agreement renewal process and submit revisions annually thereafter. Web-broker shall assume ultimate responsibility

for all services and functions described under this Agreement, including those that are subcontracted to other entities, and must ensure that subcontractors will perform all functions in accordance with all applicable requirements. Web-broker shall further be subject to such oversight and enforcement actions for functions or activities performed by subcontractor entities as may otherwise be provided for under applicable law and program requirements, including this Agreement with CMS. Notwithstanding any subcontracting of any responsibility under this Agreement, Web-broker shall not be released from any of its performance or compliance obligations hereunder, and shall remain fully bound to the terms and conditions of this Agreement as unaltered and unaffected by such subcontracting.

If Web-broker attempts to make an assignment, subcontracting arrangement 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.

c. Use of the Hub Web Services. Web-broker will only use a CMS-approved DE Environment when accessing the APIs and web services that facilitate functionality to enroll Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals' legal representatives or Authorized Representatives—through the FFEs and SBE-FPs, which includes compliance with the requirements detailed in Appendix A: Privacy and Security Standards for , Appendix B: Annual Security and Privacy Assessment (SPA), and Appendix D: Standards for Communication with the Hub.

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 ACA and the regulations codified thereunder, including as codified at 45 C.F.R. 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. Web-broker shall maintain all records that it creates in the normal course of its business in connection with activity under this Agreement for the term of this Agreement in accordance with 45 C.F.R. § 155.220(c)(3)(i)(E). 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 Web-broker's offices, and CMS's review shall not interfere unreasonably with Web-broker's business activities. This clause survives the expiration or termination of this Agreement.

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 and Consent to Jurisdiction. This Agreement will be governed by the laws and common law of the United States of America, including without limitation such regulations as may be promulgated 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 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 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, 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. Access to the FFEs and SBE-FPs. Any Web-broker; its Downstream and Delegated Entities, including downstream Agents/Brokers; 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.

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 Appendices A and B of this Agreement and the Non-Exchange Entity System Security and Privacy Plan

Printed Name and Title of Privacy Officer Attesting Compliance that Web-broker Systems Comply with Appendices A and B of this Agreement and the Non-Exchange Entity System Security and Privacy Plan

	Web-broker Partner ID
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 the benefit year as defined in Section VI.a of this Agreement:

☐ Web-broker ***will*** assist Qualified Employees and/or Qualified Employers in the benefit year as defined in this Agreement

☐ Web-broker ***will not*** assist Qualified Employees and/or Qualified Employers in the benefit year as defined in this Agreement

FOR CMS

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

Jeffrey D. Grant Deputy Director for Operations Center for Consumer Information and Insurance Oversight Centers for Medicare & Medicaid Services	**Date**
George C. Hoffmann Deputy CIO and Deputy Director Office of Information Technology (OIT) Centers for Medicare & Medicaid Services (CMS)	**Date**

Appendix A: Privacy and Security Standards for Web-brokers

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 govern any PII that is created, collected, disclosed, accessed, maintained, stored, or used by Web-brokers 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, Web-brokers agree to comply with the security and privacy standards and implementation specifications outlined in the Non-Exchange Entity System Security and Privacy Plan (NEE SSP)[8] while performing the Authorized Functions outlined in their respective Agreement(s) with CMS.

The standards documented in the NEE SSP are established in accordance with Section 1411(g) of the Affordable Care Act ("ACA") (42 U.S.C. § 18081(g)), the Federal Information Management Act of 2014 ("FISMA") (44 U.S.C. 3551), and 45 C.F.R. § 155.260 and are consistent with the principles in 45 C.F.R. §§ 155.260(a)(1) through (a)(6). All capitalized terms used herein carry the meanings assigned in Appendix C: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix C: Definitions has the meaning provided in 45 C.F.R. § 155.20.

In addition, Web-brokers must comply with the annual security and privacy assessment (SPA) requirements in Appendix B.

[8] References to security and privacy controls and implementation standards can be found in the NEE SSP located on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit.

Appendix B: Annual Security and Privacy Assessment (SPA)

Consistent with 45 C.F.R. §§ 155.220(c)(6)(iv), 155.221(b)(4)(ii) and 155.221(f), the Web-broker must contract with one or more independent Auditors to conduct an annual SPA as described below and in the ICSM Strategy Guide and the NEE SPP. All capitalized terms used herein carry the meanings assigned in Appendix C: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix C: Definitions has the meaning provided in 45 C.F.R. § 155.20.

The SPA 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) Independent Third-Party Audit. The Web-broker must contract with an independent third-party Auditor(s) with experience conducting Information system privacy and security audits to perform the SPA. The Web-broker and its Auditor(s) should refer to the Framework for Independent Assessment of Security and Privacy Controls[9] which provides an overview of the independent security and privacy assessment requirements.

The Web-broker and its Auditor(s) may reference existing audit results that address some or all of the SPA's requirements. Such existing audit results must have been generated by an independent third-party Auditor. In addition, such existing audit results must have been produced within 365 Days of completion of the SPA. If existing audit reports do not address all required elements of the SPA, the remaining elements must be addressed by an independent third-party Auditor.

(2) Assessment Methodology. The SPA methodology herein is based on the standard CMS methodology and is described in the Framework for Independent Assessment of Security and Privacy Controls. The Auditor must prepare and Web-broker must submit a Security Privacy Controls Assessment Test Plan (SAP) that describes the Auditor's scope and methodology of the assessment. Web-broker must submit the Auditor-prepared SAP at least thirty (30) Days prior to commencing the assessment. The assessment methods may include examination of documentation, logs, and configurations; interviews of personnel; and/or testing of technical controls. The SPA must 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. Web-broker security and privacy policies and procedures; and

d. Major documentation omissions and/or discrepancies.

[9] This document is located on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit.

(3) Tests and Analysis Performed. The SPA must include tests that analyze applications, systems, and associated infrastructure.[10] The tests should begin with high-level analyses and increase in specificity. Tests and analyses performed during an assessment should 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 Web-broker must develop a corrective action plan to mitigate any security and privacy risks if the SPA identifies a deficiency in the Web-broker's security and privacy controls as documented in a Plan of Action & Milestones (PO&M). Alternatively, the Web-broker may document why it believes a critical control is not applicable to its system or circumstances. The SPA results do not alter this Agreement, including any penalties for non-compliance. If the Web-broker's SPA includes findings suggesting significant security or privacy risks, and the Web-broker 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 this Agreement may be terminated for cause. In addition, CMS may delay providing final approval or may withdraw prior approval of Web-broker's DE Environment if the Web-broker does not address to the reasonable satisfaction of CMS the findings suggesting significant security or privacy risks.

(5) Non-Exchange Entity System Security Plan ("NEE SSP"). The Web-broker must implement the controls documented in the Security and Privacy Controls for Web-brokers Supplement, though, CMS strongly recommends Web-brokers participating in Classic DE implement all the NEE SSP controls.[11] The Web-broker's Auditor(s) must verify and document the Web-broker's implementation and compliance with at least the controls listed in the Security and Privacy Controls for Web-brokers Supplement. The Security Privacy Assessment Report (SAR) will be accepted by CMS as documentation of compliance with those controls so long as the assessment has been conducted within 365 Days of the completion date of the previous assessment.

(6) SPA Documentation Submission. The following table identifies the required SPA documentation that Web-Brokers must submit to CMS.

Table 1: Web-broker Privacy and Security Document Submission Requirements

[10] The Security and Privacy Controls Assessment Test Plan (SAP) Template and the Security and Privacy Assessment Report (SAR) Template provide additional guidance on testing methodology and reporting requirements. These documents are located on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit.

[11] The Security and Privacy Controls for Web-brokers Supplement will be posted at the following link on CMS zONE: https://zone.cms.gov/document/privacy-and-security-audit .

Document	Description	Submission Requirements
Security Privacy Controls Assessment Test Plan (SAP)	▪ The SAP describes the Auditor's scope and methodology of the assessment. ▪ The SAP includes an attestation of the Auditor's independence. ▪ The SAP must be completed by the Auditor and submitted to CMS for review, prior to conducting the security and privacy assessment (SPA).	▪ Submit via the Entity-specific DE/EDE PME site at least thirty (30) days before commencing the privacy and security audit; during the planning phase.
Security and Privacy Assessment Report (SAR)	▪ The report should contain a summary of findings that includes ALL findings from the assessment to include documentation reviews, control testing, scanning, penetration testing, interview(s), etc. o Explain if and how findings are consolidated. o Ensure risk level determination is properly calculated, especially when weaknesses are identified as part of the Center for Internet Security (CIS) Top 20 and/or OWASP Top 10. ▪ The assessment must be conducted by an independent third-party Auditor with experience outlined in the *Framework for Independent Assessment*. Among the experience required include familiarity with National Institute of Standards and Technology (NIST) standards, the Health Insurance Portability and Accountability Act (HIPAA), and other applicable federal privacy and cybersecurity regulations and guidance.: ▪ Alternatively, the Web-broker may reference existing audit results that address some or all of the assessment's requirements, assuming the existing audit results were produced by a third-party Auditor in conformity with the requirements described above. o If existing audit reports do not address all required elements of the assessment, the remaining elements must be addressed utilizing one of the first two assessment options. o If existing audit reports are utilized, the reports must have been based on assessment activities completed within the last year. ▪ The SAR should not include comments that describe the third-party assessor's process for verifying the requirement, unless there is a specific issue or concern with respect to the requirement that warrants raising the concern to CMS.	▪ Submit via the Entity-specific DE/EDE PME site using the SAR template on CMS zONE.[12] ▪ Only one final report should be submitted to CMS. Unless CMS has provided comments and/or requested edits to the original submission and requested a revised resubmission, no additional reports should be submitted.
Annual Penetration Testing	▪ The penetration test must include the DE Environment and must include tests based on the Open Web Application Security Project (OWASP) Top 10.	▪ Submit via the Entity-specific DE/EDE PME site with the SAR
Network and Component Vulnerability Scans	▪ A Web-broker must submit the most recent three (3) months of its Vulnerability Scan Reports. ▪ All findings from vulnerability scans are expected to be consolidated in the monthly POA&M (the POA&M is expected to be updated monthly, if applicable, but only submitted as indicated in the following row unless additional submissions are requested by CMS). ▪ Similar findings can be consolidated.	▪ Submit via web-broker's entity-specific DE/EDE PME site with the SAR
Plan of Action and Milestones (POA&M)	▪ Submit a POA&M if its third-party assessor identifies any privacy and security compliance issues in the SAR.	▪ Submit via the web-broker's entity-specific DE/EDE PME site using

[12] Documents, templates, and other materials will be posted at the following link on CMS zONE: https://zone.cms.gov/document/privacy-and-security-audit.

Document	Description	Submission Requirements
	▪ Ensure all open findings from the SAR have been incorporated into the POA&M. ▪ Explain if and how findings from the SAR were consolidated on the POA&M; include SAR reference numbers, if applicable. ▪ Ensure the weakness source references each source in detail to include type of audit/assessment and applicable date range. ▪ Ensure the weakness description is as detailed as possible to include location/server/etc., if applicable. ▪ Ensure scheduled completion dates, milestones with dates, and appropriate risk levels are included.	the POA&M template on CMS zONE with the SAR
Non-Exchange Entity System Security and Privacy Plan (NEE SSP) – if requested	▪ The NEE SSP must include complete and detailed Information about the Prospective or Existing Web-broker's implementation specifications of required security and privacy controls. ▪ The implementation of security and privacy controls must be completely documented in the SSP before the audit is initiated.	▪ Web-brokers are not required to submit the NEE SSP to CMS. However, CMS may request and review the NEE SSP. ▪ If requested to submit, Web-brokers must use the NEE SSP template on CMS zONE.
Risk Acceptance Form	▪ Ensure accepted risks are documented using the Risk Acceptance Form and submitted with the POA&M during the regular POA&M submission schedule[13].	▪ Submit via the web-broker's entity-specific DE/EDE PME site using the Risk Acceptance Form on CMS zONE with the POA&M.

(7) Submission of SPA to CMS. The Web-broker must submit the SPA electronically in a format specified by CMS during the Agreement renewal or initial onboarding process, but no later than June 30, for Existing and Prospective Web-brokers, to mitigate risk of any delay in completing the onboarding process and/or participation in the open enrollment period (OEP) as defined in Section VI.a of this Agreement. Web-brokers must submit applicable SPA documentation in accordance with the ISCM Strategy Guide throughout the term of the Agreement.

(8) CMS Review of Web-broker SPA Submission. CMS will review the Web-broker's SPA submission. If the SPA indicates that the Web-broker has not sufficiently implemented any identified required control(s), CMS will require remedial action. A Web-broker that does not submit the required SPA documentation or implement any required remedial actions may be subject to the Termination with Cause provision (Section VIII.b) of this Agreement or prohibited from executing the subsequent plan year's Agreement. In addition, CMS may delay providing final approval or may withdraw prior approval of Web-broker's DE Environment if the Web-broker does not address to the reasonable satisfaction of CMS findings suggesting significant security or privacy risks.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

[13] The *Risk Acceptance Form* is available on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit.

Appendix C: 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 C.F.R. § 155.20.

(1) **Advance Payments of the Premium Tax Credit ("APTC")** has the meaning set forth in 45 C.F.R. § 155.20.

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

(3) **Agent** or **Broker** has the meaning set forth in 45 C.F.R. § 155.20.

(4) **Agent or Broker Direct Enrollment Technology Provider** has the meaning set forth in 45 C.F.R. § 155.20.

(5) **Applicant** has the meaning set forth in 45 C.F.R. § 155.20.

(6) **Auditor** means a person or organization that meets the requirements set forth in this Agreement and contracts with a Direct Enrollment (DE) Entity for the purposes of conducting an Operational Readiness Review (ORR) in accordance with 45 C.F.R. §§ 155.220(c)(6) and 155.221(b)(4) and (f), this Agreement and CMS-issued guidance.

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

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

(9) **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 ("PII") or (2) an authorized user accesses or potentially accesses PII for anything other than an authorized purpose.

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

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

(12) **Classic Direct Enrollment ("Classic DE")** means, for the purposes of this Agreement, the original version of Direct Enrollment, which utilizes a double redirect from a Direct Enrollment (DE) Entity's website to HealthCare.gov where the eligibility application is submitted and an eligibility determination is received, and back to the DE Entity's website for Qualified Health Plan ("QHP") shopping and plan selection consistent with applicable requirements in 45 C.F.R. §§ 155.220(c)(3)(i), 155.221, 156.265 and/or 156.1230(b).

(13) **Classic Direct Enrollment Pathway ("Classic DE Pathway")** means, for the purposes of this Agreement, the application and enrollment process used by Direct Enrollment (DE) Entities for Classic DE.

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

(15) **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.

(16) **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 the Small Business Health Options Program (SHOP).

(17) **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 the Small Business Health Options Program (SHOP).

(18) **Consumer** means a person who, for himself or herself, or on behalf of another individual, seeks Information related to eligibility or coverage through a Qualified Health Plan ("QHP") offered through an Exchange 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.

(19) **Cost-sharing Reductions ("CSRs")** has the meaning set forth in 45 C.F.R. § 155.20.

(20) **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.

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

(22) **Designated Representative** means an Agent or Broker that has the legal authority to act on behalf of the Web-broker.

(23) **Direct Enrollment ("DE")** means, for the purposes of this Agreement, the process by which a Direct Enrollment (DE) Entity may assist an Applicant or Enrollee with enrolling in a QHP in a manner that is considered through the Exchange consistent with applicable requirements in 45 C.F.R. §§ 155.220(c), 155.221, 156.265, and/or

156.1230. Direct Enrollment is the collective term used when referring to both Classic Direct Enrollment and Enhanced Direct Enrollment.

(24) **Direct Enrollment ("DE") End-User Experience** means all aspects of the pre-application, application, enrollment, and post-enrollment experience and any data collected necessary for those steps or for the purposes of any Authorized Functions under this Agreement.

(25) **Direct Enrollment ("DE") Entity** has the meaning set forth in 45 C.F.R. § 155.20.

(26) **Direct Enrollment (DE) Entity Application Assisters** has the meaning set forth in 45 C.F.R. § 155.20.

(27) **Direct Enrollment ("DE") Environment** means an Information technology application or platform provided, owned, and maintained by a DE Entity through which a DE Entity establishes an electronic connection with the Hub and, utilizing a suite of CMS APIs, submits Consumer, Applicant, Qualified Individual, or Enrollee Information to the FFE for the purpose of assisting Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals' legal representatives or Authorized Representatives—in applying for APTC and/or CSRs; applying for enrollment in QHPs offered through an FFE or SBE-FP; or completing enrollment in QHPs offered through an FFE or SBE-FP.

(28) **Enhanced Direct Enrollment ("EDE")** means, for purposes of this Agreement, the version of Direct Enrollment which allows Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals' legal representatives or Authorized Representatives—to complete all steps in the application, eligibility and enrollment processes on an EDE Entity's website consistent with applicable requirements in 45 C.F.R. §§ 155.220(c)(3)(ii), 155.221, 156.265 and/or 156.1230(b) using application programming interfaces (APIs) as provided, owned, and maintained by CMS to transfer data between the Exchange and the EDE Entity's website.

(29) **Enhanced Direct Enrollment ("EDE") Entity** means a DE Entity that has been approved by CMS to use the Enhanced Direct Enrollment (EDE) Pathway.

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

(31) **Enrollee** has the meaning set forth in 45 C.F.R. § 155.20.

(32) **Exchange** has the meaning set forth in 45 C.F.R. § 155.20.

(33) **Existing Web-broker** means a Web-broker that completes the Web-broker Agreement renewal process in order to maintain its status as a Web-broker and continue operating for the plan year that occurs within the term of this Agreement.

(34) **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 ACA 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.

(35) **Health Insurance Coverage** has the meaning set forth in 45 C.F.R. § 155.20.

(36) **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 C.F.R. 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).

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

(38) **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.

(39) **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.

(40) **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.

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

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

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

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

(4) A program that makes coverage in a Qualified Health Plan ("QHP") through the Exchange with APTC established under section 36B of the Internal Revenue Code available to Qualified Individuals.

(5) A program that makes available coverage in a QHP through the Exchange with CSRs established under section 1402 of the ACA.

(42) **Issuer** has the meaning set forth in 45 C.F.R. § 144.103.

(43) **Non-Exchange Entity** has the meaning at 45 C.F.R. § 155.260(b)(1), and includes, but is not limited, to Qualified Health Plan ("QHP") Issuers, Navigators, Agents, Brokers, and Web-brokers.

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

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

(46) **Prospective Web-broker** is an entity seeking to become a Web-broker that does not have an executed Web-broker Agreement for the current plan year.

(47) **Qualified Employer** has the meaning set forth in 45 C.F.R. § 155.20.

(48) **Qualified Employee** has the meaning set forth in 45 C.F.R. § 155.20

(49) **Qualified Health Plan ("QHP")** has the meaning set forth in 45 C.F.R. § 155.20.

(50) **Qualified Health Plan ("QHP") Issuer** has the meaning set forth in 45 C.F.R. § 155.20.

(51) **Qualified Individual** has the meaning set forth in 45 C.F.R. § 155.20.

(52) **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.

(53) **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.

(54) **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.

(55) **State-based Exchange on the Federal Platform ("SBE-FP")** means an Exchange established by a State that receives approval under 45 C.F.R. § 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.

(56) **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.

(57) **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.

(58) **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.

(59) **Web-broker** has the meaning set forth in 45 C.F.R. § 155.20.

Appendix D: Standards for Communication with the Hub

The CMS Data Services Hub ("Hub") and Hub Web Services are not available for the Small Business Health Options Program (SHOP). Therefore, this Appendix is not applicable to Web-broker participation in SHOP. All capitalized terms used herein carry the meanings assigned in Appendix C: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix C: Definitions has the meaning provided in 45 C.F.R. § 155.20.

(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 Hub and the Direct Enrollment ("DE") Application Program Interfaces ("APIs") for Web-broker's own line of business.

(2) If Web-broker provides a DE Environment 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.

(3) 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.

(4) 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.

(5) 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.

(6) 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.[14]

[14] 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

(7) 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.

(8) 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.

(9) Pursuant to 45 C.F.R. §§ 155.220(c)(6), 155.221(b)(4), and 155.221(f), Web-broker must successfully complete an Operational Readiness Review ("ORR") 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 ORR 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 ORR requirements or if, at the sole discretion of CMS, the results are unsatisfactory.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

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.

Appendix E: Auditor Identification

Web-broker agrees to identify, in Part I below, all Auditors selected to complete the annual security and privacy assessment (SPA) and any subcontractors of the Auditor(s), if applicable. In the case of multiple Auditors, please indicate the role of each Auditor in completing the SPA. Include additional sheets, if necessary. All capitalized terms used herein carry the meanings assigned in Appendix C: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix C: Definitions has the meaning provided in 45 C.F.R. § 155.20.

TO BE FILLED OUT BY WEB-BROKER

I. Complete These Rows to Identify Auditors Selected to Complete SPA

Printed Name and Title of Authorized Official of Auditor 1	
Auditor 1 Business Name	
Auditor 1 Address	
Printed Name and Title of Contact of Auditor 1 (if different from Authorized Official)	
Auditor 1 Contact Phone Number	
Auditor 1 Contact Email Address	
Subcontractor Name & Information (if applicable)	
Audit Role	
Printed Name and Title of Authorized Official of Auditor 2	
Auditor 2 Business Name	
Auditor 2 Address	
Printed Name and Title of Contact of Auditor 2 (if different from Authorized Official)	
Auditor 2 Contact Phone Number	
Auditor 2 Contact Email Address	
Subcontractor Name & Information (if applicable)	
Audit Role	

Appendix F: Conflict of Interest Disclosure Form

TO BE FILLED OUT BY WEB-BROKER

Web-broker must disclose to the Department of Health & Human Services (HHS) any financial relationships between the Auditor(s) identified in Appendix E: Auditor Identification of this Agreement, and individuals who own or are employed by the Auditor(s), and individuals who own or are employed by a Web-broker for which the Auditor(s) is conducting an annual security and privacy assessment (SPA) pursuant to Appendix A: Privacy and Security Standards for Web-brokers of this Agreement and 45 C.F.R. §§ 155.220(c)(6), 155.221(b)(4), and 155.221(f). Web-broker must disclose any affiliation that may give rise to any real or perceived conflicts of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence. All capitalized terms used herein carry the meanings assigned in Appendix C: Definitions. Any capitalized term that is not defined in the Agreement, this Appendix or in Appendix C: Definitions has the meaning provided in 45 C.F.R. § 155.20.

Please describe below any relationships, transactions, positions (volunteer or otherwise), or circumstances that you believe could contribute to a conflict of interest:

☐ Web-broker has no conflict of interest to report for the Auditor(s) identified in Appendix E: Auditor Identification.
☐ Web-broker has the following conflict of interest to report for the Auditor(s) identified in Appendix E: Auditor Identification:

1. _____
2. _____
3. _____