DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
Center for Consumer Information and Insurance Oversight
200 Independence Avenue SW
Washington, DC 20201

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
CENTER FOR CONSUMER INFORMATION
& INSURANCE OVERSIGHT

Date: May 21, 2020
From: Center for Consumer Information and Insurance Oversight (CCIIO)
Title: Health Insurance Exchange Guidance
Subject: Updated Web-broker Direct Enrollment Program Participation Minimum Requirements

Updated May 21, 2020: This document has been updated since it was originally posted on December 10, 2019. This updated version replaces the prior versions of the document.

I. Background

On December 10, 2019, the Centers for Medicare & Medicaid Services (CMS) established new requirements for prospective web-brokers onboarding on or after January 1, 2020 (prospective web-brokers) and existing web-brokers that complete their Web-Broker Agreement renewal in 2020 in order to continue to operate as web-brokers for plan year (PY) 2021 (existing web-brokers) (collectively referred to as web-brokers). This guidance, which updates CMS's December 10, 2019 guidance and supersedes it, is applicable to web-brokers that operate in states using the federal platform, including Federally-facilitated Exchanges (FFEs) and State-based Exchanges on the Federal Platform (SBE-FPs) (collectively referred to as Marketplaces).

This guidance represents the minimum requirements for web-brokers participating in and seeking approval to participate in the Direct Enrollment (DE) program, whether those web-brokers are using or seeking approval to use the classic direct enrollment (classic DE) pathway only, the enhanced direct enrollment (EDE) pathway only, or both the classic DE and EDE pathways. Throughout this guidance, references to "DE," without specifying either classic DE or EDE, are inclusive of both the classic DE and EDE pathways. Note that web-brokers using or seeking to use the EDE pathway must also comply with additional requirements that are set forth in CCIIO's March 13, 2020 guidelines entitled *Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements* (EDE Guidelines),[1] and that satisfying some of the EDE-specific requirements contained therein may constitute satisfaction of some of the requirements described in this guidance.[2]

[1] The EDE Guidelines are available at: https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Guidelines-for-Third-Party-Auditors-EDE-PY20PY21-Year3.pdf.

[2] See, e.g., Section V. Considerations for Web-brokers that Are Prospective or Existing EDE Entities, of this guidance for specific information on how the requirements may impact web-brokers approved for or seeking to be approved for EDE.

Pursuant to 45 C.F.R. § 155.221(b)(4), DE Entities,[3] including web-brokers, must demonstrate operational readiness and compliance with applicable requirements prior to their websites being used to complete an Exchange eligibility application or qualified health plan (QHP) selection. Web-brokers must also comply with the privacy and security standards set forth in Appendix A: Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities in the *Agreement between Web-broker and the Centers for Medicare & Medicaid Services for the Federally-facilitated Exchanges and State-based Exchanges on the Federal Platform* (Web-broker Agreement) and the *Non-Exchange Entity System Security and Privacy Plan* (NEE SSP).[4] Further details are provided in Exhibit 1.

Exhibit 1. Privacy and Security Requirements for Web-brokers

Requirement	Description
Privacy and Security Control Implementation	▪ Web-brokers must implement the security and privacy controls[5] in the Web-broker Agreement consistent with the corresponding implementation standards in the NEE SSP to participate in classic DE.[6] – These controls include the "critical security and privacy controls" noted via control abbreviations in Appendix A subsection: Annual Security and Privacy Attestation (SPA) of the Web-broker Agreement, as well as controls that are represented in provisions throughout the Web-broker Agreement but are not identified with control abbreviations. Appendix A of this guidance maps all the relevant NEE SSP controls in the Web-broker Agreement. – The NEE SSP contains comprehensive security and privacy controls and implementation standards for all aspects of the DE program. Therefore, the NEE SSP contains security and privacy controls and implementation standards for the controls that web-brokers must implement from the Web-broker Agreement, as well as additional controls and implementation standards that CMS strongly recommends web-brokers participating in classic DE implement.[7] ▪ Web-brokers are required to assess the controls in the Web-broker Agreement, per Appendix A subsection: Annual Security and Privacy Attestation (SPA) of the Web-broker Agreement. – Appendix A describes the annual assessment that web-brokers must conduct, including the assessment methodology, tests and analysis to be performed, and the critical security and privacy controls that must be evaluated on an annual basis.[8]

As discussed in more detail in the following sections, as of January 1, 2020, web-brokers are required to submit privacy and security-related documentation demonstrating that they have complied with current requirements in the Web-broker Agreement and applicable regulations. In addition, they are required to respond to an annual data request and may be required to complete additional testing. Prospective web-brokers are also required to undergo a pre-approval website review that will occur before their respective websites can go live and be made available to consumers.

[3] DE Entities are web-brokers and QHP issuers that are permitted to assist consumers with direct enrollment in QHPs offered through the Marketplaces and that meet the applicable requirements contained in 45 C.F.R. § 155.221, and either 45 C.F.R. § 155.220 or 45 C.F.R. § 156.1230, respectively. See 45 C.F.R. § 155.221(a). This guidance, however, is only applicable to web-brokers.

[4] See also 45 C.F.R. §§ 155.220(d)(3) and 155.260(b).

[5] As detailed in Section V. Considerations for Web-brokers that Are Prospective or Existing EDE Entities, of this guidance, additional privacy and security controls apply to web-brokers participating in EDE.

[6] The Web-broker Agreement, NEE SSP, and other documents are available on CMS zONE at the following link: https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials.

[7] See footnote 5.

[8] See footnote 5.

II. Updated Operational Readiness Review Business Requirements as of January 1, 2020

Web-brokers are required to comply with the following updated business requirements:

- **Annual data request**: This includes providing licensure information, points of contact, third-party relationships, and other related data elements to CMS.
- **Testing, including renewal testing** (if applicable): Existing web-brokers that have not enrolled consumers using their DE websites in the past year, as well as all prospective web-brokers, must complete testing with the CMS Data Services Hub (Hub) prior to renewing or executing their Web-broker Agreements. The ability to successfully complete an enrollment via the EDE pathway, as demonstrated during testing required to receive approval to use the EDE pathway, satisfies this requirement.

Both the annual data request and testing requirements, if applicable, are required as part of the initial onboarding for prospective web-brokers or as part of the annual renewal process for existing web-brokers.

- **Web-broker Agreement**: The Web-broker Agreement is effective from execution through the day before the first day of the following annual open enrollment period (OEP)[9] and must be re-signed annually. Web-brokers must submit the signed Web-broker Agreement to maintain or obtain their Hub-issued Partner ID and must have a countersigned agreement to maintain access to the DE application programming interfaces (APIs) in production.

  CMS will e-mail Web-broker Agreement renewal instructions and materials (including the data request and a copy of the next plan year's Web-broker Agreement) to existing web-brokers prior to the annual OEP. CMS will identify and notify existing web-brokers that must complete renewal testing in advance of the OEP. This notification will include the renewal testing instructions.

  Prospective web-brokers will receive an e-mail from CMS with Web-broker Agreement execution instructions and materials (including the data request, a copy of the applicable plan year's Agreement, and testing instructions) as part of the onboarding process. Prospective web-brokers will build their DE websites and complete technical onboarding (including the pre-approval website review – see below for more information) prior to receiving a countersigned Web-broker Agreement from CMS. After an initial interview, prospective web-brokers will submit the signed Web-broker Agreement to CMS and receive access to DE technical materials on CMS zONE and a Hub-issued Partner ID for testing purposes only; the Partner ID will only be activated in production after CMS countersigns the Web-broker Agreement.[10]

- **Testing Environment**: Web-brokers must maintain testing environments that accurately represent their DE production environments. For prospective web-brokers, their testing environments must reflect their prospective DE production environments. CMS will conduct ongoing oversight of web-brokers, including regular reviews of web-broker websites for compliance with website display requirements and guidance.

[9] See 45 C.F.R. § 155.410(e).

[10] Web-broker DE documents and materials will be posted at the following link on CMS zONE: https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials.

Prospective web-brokers must also comply with the following updated onboarding requirement:

- **Pre-approval Website Review:** Prospective web-brokers must pass a website review before having their Hub-issued Partner IDs activated in production. CMS will review prospective web-brokers' websites to ensure compliance with DE website display requirements and guidance.
  - The prospective web-broker is required to provide CMS, via DE Support, with a set of credentials that CMS can use to access the entity's DE website testing environment (i.e., pre-production environment) to complete the website review of the entity's DE environment. The prospective web-broker must ensure that the testing credentials are valid and that all APIs and components of its DE implementation in its website testing environment are accessible for the duration of the review. CMS will request test credentials from prospective web-brokers as part of the onboarding process.

Additional information related to the web-broker onboarding process is detailed on CCIIO's website in the *Processes and Guidelines for Becoming a Web-broker in the Federally-facilitated Exchanges*, accessible from the following webpage: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Web-brokers-in-the-Health-Insurance-Marketplace.

III. Operational Readiness Review Privacy and Security Documentation Requirements That Took Effect on January 1, 2020

As of January 1, 2020, web-brokers were no longer required to use the self-attestation in Appendix D: Annual Security and Privacy Attestation Report of the Web-broker Agreement to document completion of the annual assessment. To demonstrate compliance with the requirements in Appendix A of the Web-broker Agreement, web-brokers are now required to submit the complete set of documents outlined in Exhibit 2 to CMS, except as noted in the "Submission Requirements" column.[11] All assessment activities that serve as the basis for the documentation in Exhibit 2 must have been completed within the last year. See Section IV. Deadlines and Final Approval, of this guidance for details on the timing and deadline for submission of this documentation.

Exhibit 2. Required Privacy and Security Documentation

Document	Description	Submission Requirements
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 secure portal with the SAR[12]

[11] These documents may also be requested from web-brokers who currently participate in DE as part of a CMS review or audit to assess the web-broker's compliance with applicable requirements. See, e.g., 45 C.F.R. §§ 155.220(c)(5) and 155.221(f)(7). There are also additional privacy and security documentation requirements for web-brokers using or intending to use the EDE pathway. See the EDE Guidelines referenced in footnote 1 and Section V. Considerations for Web-brokers that Are Prospective or Existing EDE Entities of this guidance for more information.

[12] Web-brokers that do not already have a secure portal account must e-mail DE Support at directenrollment@cms.hhs.gov to receive instructions to create an account at the time they are ready to submit the requested documentation. CMS will not require web-brokers to encrypt documents containing proprietary information before uploading them to the portal.

Document	Description	Submission Requirements
Security and Privacy Assessment Report (SAR) – (third-party auditor preferred)	▪ 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. – Explain if and how findings are consolidated. – 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. ▪ Assessment options: The report may be prepared by: – A third-party auditor (recommended); or – Internal staff, provided that: o They have appropriate qualifications to evaluate security and privacy controls. The internal staff should be familiar 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. In addition, the internal staff should be capable of performing penetration testing and vulnerability scans. o They are not involved in the developmental, operational, and/or management chain associated with the system that is the subject of the assessment. ▪ 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 or internal staff in conformity with the requirements described above. – 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. – 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 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 secure portal using the SAR template on CMS zONE[13] ▪ 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.
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 the secure portal with the SAR
Plan of Action and Milestones (POA&M)	▪ Submit a POA&M if its assessor identifies any privacy and security compliance issues in the SAR.	▪ Submit via the secure portal using the POA&M template on

[13] Documents, templates, and other materials will be posted at the following link on CMS zONE: https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials.

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.	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.	▪ 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.

IV. Deadlines and Final Approval

Web-brokers must submit the privacy and security documentation discussed in Section III, Operational Readiness Review Privacy and Security Documentation Requirements That Took Effect on January 1, 2020, as soon as possible during their respective renewal or onboarding processes, but no later than September 15, 2020, to mitigate risk of any delay in completing the onboarding process and/or participating in the plan year 2021 OEP.[14] Web-brokers that submit the required documentation after September 15, 2020 may not be approved in time to operate during the plan year 2021 OEP. Exhibit 3 contains additional details regarding the privacy and security documentation submission options and deadlines that exist for web-brokers who are prospective or existing EDE Entities.

Web-brokers must also meet the updated operational readiness review business requirements in Section II, Updated Operational Readiness Review Business Requirements as of January 1, 2020, as part of the web-broker onboarding or renewal processes, as applicable.

[14] Throughout Section IV and Section V of this guidance, September 15, 2020 is cited as the deadline by which web-brokers must submit certain privacy and security documentation insofar as a web-broker intends to operate during the OEP for plan year 2021. If a web-broker does not intend to operate during the plan year 2021 OEP, the web-broker does not have a specific deadline for submitting the privacy and security documentation; however, the web-broker will not be approved to go live with a DE environment until the privacy and security documentation described in this guidance has been submitted to CMS and CMS has reviewed and approved the documentation. CMS requires time to review the documentation prior to approving the web-broker; accordingly, web-brokers should not wait until they are ready to go live to submit the privacy and security documentation.

CMS will review all submitted materials and contact web-brokers with any questions or requests for further documentation. CMS does not guarantee onboarding or renewal timeframes. CMS will notify web-brokers once their privacy and security documents are deemed complete and once these entities have met all other requirements in this guidance. Existing web-brokers who fail to meet all applicable requirements in this guidance will not be permitted to renew their Web-broker Agreement until they have met these requirements. Prospective web-brokers must submit the privacy and security documentation and comply with the applicable updated operational readiness review business requirements prior to receiving a countersigned Web-broker Agreement from CMS and being approved to use either of the DE pathways.

V. Considerations for Web-brokers that Are Prospective or Existing EDE Entities

A. Overview for All Web-brokers

A web-broker that is using or seeking to use the EDE pathway must meet the applicable web-broker operational readiness review requirements detailed in this guidance. For example, all web-brokers, including prospective or existing EDE Entities, are required to respond to the annual data request, conduct Hub testing (if applicable), execute the Web-broker Agreement, and maintain a testing environment, and all prospective web-brokers, including prospective EDE Entities, are required to undergo a pre-approval website review.

However, the EDE program also has its own set of requirements that a prospective EDE Entity must meet to be approved, or that an existing EDE Entity must meet to maintain approval. A prospective web-broker must satisfy the requirements in this guidance and receive CMS approval to be a web-broker prior to being approved to be an EDE Entity,[15] which it may do prior to or concurrent with completion of EDE program requirements. For more information on the business requirements and privacy and security requirements that a prospective EDE Entity must meet to be approved to use the EDE pathway, please refer to the EDE Guidelines.[16] For example, the business requirements for the EDE pathway include developing an application user interface, integrating with the EDE APIs, developing post-eligibility application communications for consumers, and implementing identity proofing for consumers and agents and brokers.

Prospective or existing web-brokers that intend to seek approval to participate in EDE or that are currently approved to use EDE should consider how the privacy and security requirements outlined in this guidance may be relevant in the context of the assessments they intend to complete or have completed with respect to EDE. The SAR and POA&M templates referenced in this guidance are nearly identical to the templates that EDE Entities must submit to CMS as part of their privacy and security audits to be approved to participate in EDE. However, web-brokers seeking to participate in EDE must implement all the security and privacy controls documented in the NEE SSP. While CMS strongly recommends all web-brokers implement all of the controls in the NEE SSP, web-brokers only participating in classic DE are only required to implement and assess the controls documented in the Web-broker Agreement (see Appendix A), which are a subset of the controls in the NEE SSP. Therefore, web-brokers approved or seeking

[15] See the EDE Guidelines referenced in footnote 1 for more information about different ways to participate in the EDE program (specifically, see Section IV, Critical Decision Factors, of the EDE Guidelines).

[16] See the EDE Guidelines referenced in footnote 1 (specifically, see Section VI, Business Audit Requirements and Scope, and Section VII, Privacy and Security Audit Requirements and Scope, of the EDE Guidelines) for more information.

approval to participate in EDE may not need to complete a separate assessment as documented in this guidance as long as their assessments for purposes of EDE approval include all classic DE environments and functionality, and include assessment of all controls documented in the NEE SSP, consistent with this guidance.[17] Under certain conditions detailed below, CMS will accept an attestation from a web-broker that asserts that its EDE privacy and security audit conducted by an independent, third-party auditor addresses the web-broker's compliance with the web-broker privacy and security documentation requirements in this guidance. In such a case, the web-broker's privacy and security audit documentation will be or would have been reviewed and approved by CMS as part of its EDE approval or Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide processes.

Exhibit 3 provides a high-level overview of select example scenarios and documentation submission options for satisfying the web-broker privacy and security documentation requirements in this guidance by EDE Entity type and scope of EDE privacy and security audit. After the table, Sections V.B, Overview for Web-brokers that Are Existing (Approved) EDE Entities, and V.C, Overview for Web-brokers that Are Prospective EDE Entities, provide more details on the privacy and security documentation requirement considerations for web-brokers that are also submitting EDE privacy and security audits.

Exhibit 3. Select Example Scenarios of Documentation Submission Options for Web-broker Privacy and Security Requirements Based on EDE Entity Type and Scope of EDE Privacy and Security Audit

Example Scenario	EDE Entity Type[18]	Scope of EDE Privacy and Security Audit	Web-broker Privacy and Security Documentation Requirements Options	Deadline(s) for Calendar Year 2020 for Approval Before OEP (dates subject to change in subsequent years)
1	**Existing primary EDE Entity, including Existing EDE Entities changing application phases[19]**	▪ EDE environment and functionality assessed within the last year (based on the date documented in the SAR), but the assessment was not inclusive of all classic DE environments and functionality[20]	1) Assess whether the scope of its EDE Entity privacy and security audit covered a portion of the web-broker privacy and security requirements in this guidance and if so, submit the EDE ISCM with supplemental audit documentation related to the assessed web-broker privacy and security audit	1) August 30, 2020 2) September 15, 2020

[17] Web-brokers that are prospective or existing EDE Entities should contact DE Support (directenrollment@cms.hhs.gov) if they are unsure whether another assessment is necessary.

[18] Existing and prospective EDE Entities, for purposes of this guidance, refer to the EDE Entity's status with respect to its privacy and security audit. For example, an existing EDE Entity has had an initial EDE privacy and security audit reviewed and approved by CMS, and a prospective EDE Entity has not had a privacy and security audit approved by CMS.

[19] A primary EDE Entity is an entity that develops, designs, and hosts its own EDE environment for its own use or for use by others; please refer to the EDE Guidelines referenced in footnote 1 for more information.

[20] If a web-broker does not maintain a classic DE environment, please refer to the attestation processes defined below for existing EDE Entities in Section V.B.

			requirements that were not previously assessed and submit an attestation consistent with Section V of this guidance; OR 2) Submit web-broker privacy and security documentation consistent with this guidance	
2	**Existing primary EDE Entity, including existing EDE Entities changing application phases**	▪ EDE and classic DE environments and functionality assessed within the last year (based on the date documented in the SAR)	1) Verify that the scope of its EDE Entity privacy and security audit covered all of the web-broker privacy and security requirements in this guidance and if so, submit attestation to CMS consistent with Section V of this guidance	1) September 15, 2020
3	**Existing hybrid, non-issuer upstream EDE Entity**[21]	▪ EDE environment and functionality assessed within the last year (based on the date documented in the SAR), but the assessment was not inclusive of all classic DE environments and functionality	1) Assess whether the scope of its hybrid, non-issuer upstream EDE Entity privacy and security audit covered a portion of the web-broker privacy and security requirements in this guidance and if so, submit the EDE ISCM with supplemental audit documentation related to the assessed web-broker privacy and security audit requirements that were not previously assessed and submit an attestation consistent with Section V of this guidance; OR 2) Submit web-broker privacy and security documentation consistent with this guidance	1) August 30, 2020 2) September 15, 2020

[21] Hybrid, non-issuer upstream EDE Entities are one type of upstream EDE Entity arrangement that may be primarily characterized by the presence of additional functionality or systems to the primary EDE Entity's EDE environment beyond minor branding changes; please refer to the EDE Guidelines referenced in footnote 1 for more information.

4	**Existing hybrid, non-issuer upstream EDE Entity**	▪ EDE and classic DE environments and functionality assessed within the last year (based on the date documented in the SAR)	1) Verify that the scope of its hybrid, non-issuer upstream EDE Entity privacy and security audit covered all of the web-broker privacy and security requirements in this guidance and if so, submit an attestation consistent with Section V of this guidance; this scenario also applies to web-brokers that are not operating a classic DE environment or utilizing classic DE functionality.	1) September 15, 2020
5	**Prospective primary EDE Entity**	▪ EDE environment and functionality assessed within the last year (based on the date documented in the SAR), but the assessment was not inclusive of all classic DE environments and functionality[22]	1) If the web-broker plans to submit or has submitted its initial privacy and security audit during the 2020 audit submission window, assess whether the scope of its EDE Entity privacy and security audit covered a portion of the web-broker privacy and security requirements in this guidance and if so, revise the EDE privacy and security audit documentation as needed to document a supplemental assessment of web-broker privacy and security audit requirements that were not previously assessed and submit or resubmit the revised audit prior to the close of the audit submission window along with an attestation consistent with Section V of this guidance; OR 2) If the web-broker is newly approved to use the EDE pathway prior	1) July 31, 2020 2) August 30, 2020 3) September 15, 2020

[22] If a web-broker does not intend to maintain a classic DE environment, please refer to the attestation processes defined below for prospective EDE Entities in Section V.C.

			to August 2020 and has not already submitted its 2020 ISCM audit documentation, assess whether the scope of its EDE Entity privacy and security audit covered a portion of the web-broker privacy and security requirements in this guidance and if so, submit the EDE ISCM with supplemental audit documentation related to the assessed web-broker privacy and security audit requirements that were not previously assessed and submit an attestation consistent with Section V this guidance; OR 3) Submit web-broker privacy and security documentation consistent with this guidance	
6	**Prospective primary EDE Entity**	▪ EDE and classic DE environments and functionality assessed within the last year (based on the date documented in the SAR)	1) Verify that the scope of its EDE Entity privacy and security audit covered all of the web-broker privacy and security requirements in this guidance and if so, submit the EDE privacy and security audit and an attestation consistent with Section V of this guidance; OR 2) Submit web-broker privacy and security documentation consistent with this guidance	1) July 31, 2020 2) September 15, 2020
7	**Prospective hybrid, non-issuer**	▪ EDE environment and functionality	1) Assess whether the scope of its hybrid,	1) September 15, 2020[23]

[23] While the initial audit submission for a prospective hybrid, non-issuer upstream EDE Entity does not have a deadline, if the web-broker is relying on its EDE privacy and security audit to satisfy the web-broker privacy and security documentation requirements in this guidance, then—as described in Section IV of this guidance—the web-broker must submit web-broker privacy and security documentation by September 15, 2020 consistent with this

	upstream EDE Entity	assessed within the last year (based on the date documented in the SAR), but the assessment was not inclusive of all classic DE environments and functionality	non-issuer upstream EDE Entity privacy and security audit covered only a portion of the web-broker privacy and security requirements in this guidance and if so, submit the supplemental audit documentation related to the assessed web-broker privacy and security audit requirements that were not previously assessed and submit an attestation consistent with Section V of this guidance; OR 2) Submit web-broker privacy and security documentation consistent with this guidance	2) September 15, 2020
8	**Prospective hybrid, non-issuer upstream EDE Entity**	▪ EDE and classic DE environments and functionality assessed within the last year (based on the date documented in the SAR)	1) Verify that the scope of its hybrid, non-issuer upstream EDE Entity privacy and security audit covered all the web-broker privacy and security requirements in this guidance and if so, submit an attestation consistent with Section V of this guidance; this also applies to web-brokers that are not operating a classic DE environment or utilizing classic DE functionality.	1) September 15, 2020[24]

B. *Overview for Web-brokers that Are Existing (Approved) EDE Entities*

Overview of the privacy and security documentation process for a web-broker that is an **Existing (Approved) EDE Entity** (applies to existing primary EDE Entities; existing primary EDE Entities that are pursuing an application phase change; and existing hybrid, non-issuer upstream EDE Entities):

guidance to remain a classic DE web-broker. In these circumstances, failure to submit sufficient privacy and security documentation by September 15, 2020 may result in termination or expiration without renewal of the web-broker's Web-broker Agreement.

[24] See footnote 23.

1) A web-broker that is an existing EDE Entity may use its original EDE privacy and security audit or its most recent EDE ISCM Strategy Guide submission to demonstrate compliance with the web-broker privacy and security documentation requirements described in Exhibit 2 of this guidance if the EDE privacy and security audit or the most recent EDE ISCM Strategy Guide submission: 1) assessed the web-broker's classic DE environments and functionality, and 2) was completed within the past year.

   a) Note: A web-broker that is an existing hybrid, non-issuer upstream EDE Entity may use its original EDE privacy and security audit or its most recent EDE ISCM Strategy Guide submission to demonstrate full or partial compliance with the web-broker privacy and security documentation requirements described in Exhibit 2 of this guidance if the EDE privacy and security audit or the most recent EDE ISCM Strategy Guide submission: 1) assessed the web-broker's classic DE environments and functionality and 2) was completed in the past year. In order for this EDE submission to demonstrate full compliance with the web-broker privacy and security documentation requirements described in this guidance, the EDE privacy and security audit or ISCM Strategy Guide submission must have assessed the web-broker's implementation of the full set of the required web-broker privacy and security controls defined in Appendix A (i.e., the web-broker did not rely on the primary EDE Entity's inheritable EDE privacy and security controls to meet any of the web-broker privacy and security controls defined in Appendix A). Otherwise, the EDE privacy and security audit submission would demonstrate partial compliance with the requirements in this guidance. In that case, the web-broker must submit a supplemental privacy and security documentation package demonstrating its compliance with the web-broker privacy and security controls that the web-broker has not assessed as part of its EDE privacy and security audit submission.

   b) If a web-broker intends to use its EDE privacy and security audit or EDE ISCM Strategy Guide submission to satisfy some or all of the web-broker privacy and security documentation requirements, and the stipulated conditions to leverage this option are met, the web-broker must submit an attestation to DE Support[25] that states that some or all of its classic DE environments and functionality were assessed in its EDE privacy and security audit or EDE ISCM Strategy Guide submission completed by a third-party auditor. The attestation must be submitted on company letterhead and must be signed and dated by an authorized company representative. Existing web-brokers that assert their EDE assessments included some or all classic DE environments and functionality may be required to submit evidence in support of that assertion if CMS does not already possess the relevant artifacts (e.g., an NEE SSP).

2) Alternatively, if a web-broker does not maintain a classic DE environment and functionality, and has otherwise met the web-broker privacy and security requirements with its EDE environment implementation and associated privacy and security audit, the web-broker may use its EDE privacy and security documentation and approval status to satisfy the web-broker privacy and security documentation requirements in this guidance. If a web-broker intends to exercise this option for satisfying the web-broker privacy and security documentation requirements, consistent with the processes defined in this section, the web-broker must

[25] The web-broker may accomplish this by submitting the attestation to the DE Support at directenrollment@cms.hhs.gov.

submit an attestation—consistent with the processes and standards defined in Section V.B, item 1.b above—by September 15, 2020 that states that the web-broker does not maintain classic DE environments and functionality. This process is permissible for web-brokers that 1) do not maintain a classic DE environment and 2) have met applicable EDE privacy and security requirements and that CMS has approved as a primary EDE Entity or as a hybrid, non-issuer upstream EDE Entity.[26]

3) If the original EDE privacy and security audit or the most recent EDE ISCM Strategy Guide submission did not assess the web-broker's classic DE environments and functionality, the web-broker can assess and document the relevant web-broker privacy and security controls—defined in Appendix A—for its classic DE environments and functionality in its next ISCM submission, which must be submitted to CMS by August 30, 2020.

   a) Note: Additionally, if an existing hybrid, non-issuer upstream EDE Entity relied on a primary EDE Entity's inheritable controls for one or more required web-broker controls (regardless of whether the web-broker assessed the classic DE environments and functionality in its original submission), the hybrid, non-issuer upstream EDE Entity can assess and document the relevant web-broker privacy and security controls for its classic DE environments and functionality in its next ISCM submission, which must be submitted to CMS by August 30, 2020. In this scenario, the web-broker may only rely on its primary EDE Entity's implementation of an inheritable control for the purpose of EDE participation. If the web-broker maintains its own classic DE environment and functionality, then the web-broker must submit documentation that demonstrates assessment of all controls in Appendix A of this guidance for its classic DE environment and functionality consistent with one of the options described in this section. If a web-broker is not maintaining its own classic DE environment and functionality, please refer to Section V.B, item 2 above for the applicable requirements.

   b) If a web-broker intends to use its EDE ISCM Strategy Guide submission to satisfy some or all of the web-broker privacy and security documentation requirements in this guidance, the web-broker must submit an attestation to DE Support[27] that states that some or all of its classic DE environments and functionality were assessed in its EDE ISCM Strategy Guide submission completed by a third-party auditor. The attestation must be submitted on company letterhead and must be signed and dated by an authorized company representative. Existing web-brokers that assert their EDE assessments included some or all classic DE environments and functionality may be required to submit evidence in support of that assertion if CMS does not already possess the relevant artifacts (e.g., an NEE SSP).

[26] All assessment activities that serve as the basis for satisfaction of the privacy and security documentation requirements in this guidance must have been completed within the last year.

[27] The web-broker may accomplish this by submitting the attestation to the DE Support at directenrollment@cms.hhs.gov.

C. *Overview for Web-brokers that Are Prospective EDE Entities*

Overview of the privacy and security documentation process for a web-broker that is a **Prospective EDE Entity** (applies to both primary EDE Entities and hybrid, non-issuer upstream EDE Entities):

1) A web-broker that submits an EDE privacy and security audit in an EDE audit submission window[28] may be able to use that privacy and security audit to demonstrate compliance with the web-broker privacy and security documentation requirements described in Exhibit 2 of this guidance if the EDE privacy and security audit: 1) assessed the web-broker's classic DE environments and functionality, and 2) was completed within the past year.

    a) Note: A web-broker that submits an EDE privacy and security audit as a prospective hybrid, non-issuer upstream EDE Entity may be able to use that privacy and security audit to demonstrate full or partial compliance with the web-broker privacy and security documentation requirements described in Exhibit 2 of this guidance if the EDE privacy and security audit: 1) assessed the web-broker's classic DE environments and functionality and 2) was completed in the past year. In order for the EDE submission to demonstrate full compliance with the web-broker privacy and security documentation requirements described in this guidance, the EDE privacy and security audit must have assessed the web-broker's implementation of the full set of web-broker privacy and security controls defined in Appendix A (i.e., the web-broker did not rely on the primary EDE Entity's inheritable EDE privacy and security controls to meet any of the web-broker privacy and security controls that web-brokers must document consistent with the requirements in Exhibit 2 of this guidance). Otherwise, the EDE privacy and security audit submission would demonstrate partial compliance with the requirements in this guidance. In that case, the web-broker must submit a supplemental privacy and security documentation package demonstrating its compliance with the web-broker privacy and security controls that the web-broker has not assessed as part of its EDE privacy and security audit submission.

    b) If a prospective hybrid, non-issuer upstream EDE Entity relied on a primary EDE Entity's inheritable controls for one or more required web-broker controls (regardless of whether the web-broker assessed the classic DE environments and functionality in its EDE audit submission), the web-broker may only rely on its primary EDE Entity's implementation of an inheritable control for the purpose of EDE participation. If the web-broker maintains its own classic DE environment and functionality, then the web-broker must submit documentation that demonstrates assessment of all controls in Appendix A of this guidance for its classic DE environment and functionality consistent with one of the options described in this section. If a web-broker is not maintaining its own classic

[28] The EDE audit submission window in 2020 began on April 1, 2020 and was originally set to end on June 30, 2020. However, on April 9, 2020, CMS issued guidance extending the deadline by which prospective primary EDE Entities interested in implementing EDE and existing primary EDE Entities seeking to change phases in calendar year 2020 must submit business requirements and privacy and security audits to July 31, 2020 due to the public health emergency posed by COVID-19. See https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Notice-of-Updated-2020-EDE-Audit-Submission-Deadline.pdf for more information on the extended audit submission deadline.

DE environment and functionality, please refer to Section V.C, item 2 below for the applicable requirements.

c) A web-broker that is submitting an initial EDE privacy and security audit as a prospective hybrid, non-issuer upstream EDE Entity may submit the EDE privacy and security audit at any time (i.e., outside of the audit submission window); however, if the web-broker is relying on this hybrid, non-issuer upstream EDE Entity privacy and security audit to satisfy the web-broker privacy and security documentation requirements in this guidance, the web-broker must submit privacy and security documentation by September 15, 2020, consistent with this guidance to remain a classic DE web-broker. As described in Section IV of this guidance, failure to do so may result in termination or expiration without renewal of the web-broker's Web-broker Agreement.

d) If a web-broker intends to use its EDE privacy and security audit to satisfy some or all of the web-broker privacy and security documentation requirements in this guidance, and the stipulated conditions to leverage this option are met, the web-broker can submit an attestation that states that some or all of its classic DE environments and functionality were assessed in the EDE privacy and security audit completed by a third-party auditor. The attestation must be submitted on company letterhead and must be signed and dated by an authorized company representative. Existing web-brokers that assert their EDE assessments included some or all classic DE environments and functionality may be required to submit evidence in support of that assertion if CMS does not already possess the relevant artifacts (e.g., an NEE SSP).

2) Alternatively, if a web-broker does not maintain a classic DE environment and functionality, and has otherwise met the web-broker privacy and security requirements with its EDE environment implementation and associated audit, the web-broker may use its EDE privacy and security documentation and approval status to satisfy the web-broker privacy and security documentation requirements in this guidance. If a web-broker intends to exercise this option for satisfying the web-broker privacy and security documentation requirements, consistent with the processes defined in this section, the web-broker must submit an attestation—consistent with the processes and standards defined in Section V.C, item 1.d above—by September 15, 2020 that states that the web-broker does not maintain classic DE environments and functionality. This process is permissible for web-brokers that 1) do not maintain a classic DE environment and 2) have met applicable EDE privacy and security requirements and that CMS has approved as a primary EDE Entity or as a hybrid, non-issuer upstream EDE Entity.[29]

3) For a prospective primary EDE Entity that is submitting a privacy and security audit during the audit submission window that includes the privacy and security documentation necessary to meet the requirements in this guidance, the EDE privacy and security audit documentation (using the EDE templates) must be deemed "complete" by CMS to be used for both EDE approval and to satisfy the requirements described in this guidance.[30] CMS will not accept rejected, incomplete EDE privacy and security audit documentation as the basis to satisfy the

[29] All assessment activities that serve as the basis for satisfaction of the privacy and security documentation requirements in this guidance must have been completed within the last year.

[30] Please see Section X.C. of the EDE Guidelines referenced in footnote 1 for the minimum requirements for a complete EDE privacy and security audit.

web-broker privacy and security documentation requirements described in Exhibit 2 of this guidance.

a) If the EDE audit is deemed incomplete or rejected *within the audit submission window*, the web-broker and its Auditor may revise the documentation (within the EDE templates) consistent with CMS feedback and re-submit it to CMS prior to July 31, 2020. If, at that point, the EDE privacy and security audit is deemed complete, the audit will be added to the review queue to evaluate compliance with the privacy and security documentation requirements described in Exhibit 2 of this guidance prior to approval.

b) If the EDE audit is deemed incomplete or rejected after *the audit submission window has closed*, the web-broker and its Auditor may still revise the documentation consistent with CMS feedback[31] and resubmit the documentation to satisfy the web-broker privacy and security documentation requirements described in Exhibit 2 of this guidance prior to September 15, 2020. However, the audit may not be resubmitted after July 31, 2020 for purposes of EDE approval as a primary entity.[32] The web-broker does not need to switch to the NEE SSP template prior to resubmitting this documentation. CMS will evaluate the revised submission against the standards described in Exhibit 2 of this guidance. In this scenario, the web-broker will not be able to pursue approval to participate in the EDE program as a primary EDE entity until the following year's audit submission window because its EDE privacy and security audit submission was rejected as incomplete after the audit submission window ended.

Web-brokers that are prospective or existing EDE Entities should contact DE Support (directenrollment@cms.hhs.gov) if they are unsure whether another assessment is necessary.

VI. Resources

A. Help Desk

In addition to hosting weekly webinars, which include time for interactive questions and answers, CMS currently manages multiple DE Entity-facing help desks to address questions; help DE Entities and prospective DE Entities resolve technical problems, operational issues, and other issues; and respond to policy questions. An entity must either remove personally identifiable information (PII) in documents before sending them to the help desks or encrypt the e-mail transmitting the PII.

- DE Entities with technical issues or questions that concern their technical build or system issues identified in the test or production environment should e-mail the FEPS Help Desk at CMS_FEPS@cms.hhs.gov with the subject line "DE: Tech Q for [Partner] on [Topic]."
- DE Entities with technical questions related to Hub onboarding for DE in general, Hub onboarding for the various DE APIs, and connectivity issues related to accessing the DE APIs may alternatively e-mail the Hub Help Desk at dsh.support@qssinc.com with the subject line "DE: API Q for [Partner] on [Topic]." E-mails to the FEPS Help Desk and Hub Help Desk will be routed to the appropriate team.

[31] This refers to the feedback that served as the basis for CMS's rejection of the audit for purposes of EDE approval as a primary entity.

[32] Hybrid, non-issuer upstream EDE Entity audit submissions are not subject to the audit submission window.

For a timely response, the DE Entity representative submitting the question should ensure that e-mails to the FEPS Help Desk and Hub Help Desk include the following information:

- Contact information (e-mail and phone number).
- Name of organization and organization's CMS-issued Partner ID.
- At the top of the e-mail, please summarize whether the e-mail concerns a DE technical question, testing issue, or production issue, where possible. Additionally, please note the environment where the issue was encountered, if applicable. This summary will enable the Help Desk to route the e-mail to the right subject matter expert for a more efficient response.
- If reporting on a technical issue encountered in production or while testing DE, please include the request/response XMLs/JSONs for troubleshooting (API requests and responses). DE Entities must remove PII prior to sending the XML/JSON to the FEPS Help Desk or Hub Help Desk or the DE Entity must encrypt the e-mail.

A DE Entity with a policy and compliance question related to the privacy and security assessment or Web-broker Agreement should e-mail DE Support at directenrollment@cms.hhs.gov with the subject line "Web-broker Q for [Partner] on [Topic]."

B. Webinars

CMS presents important DE updates through the Issuer Technical Workgroup (ITWG) webinar weekly on Tuesdays from 3:00 PM to 4:30 PM ET. The ITWG call is open to all web-brokers and issuers operating on the federal platform. CMS will continue to use the ITWG call to update the DE community on developments related to DE and offer interactive question and answer time at the end of each session.

To obtain the call-in information for the weekly ITWG webinar, users must register via a one-time Webinar Registration URL for the ITWG meeting series. This URL can be found on CMS zONE.[33] Note: If you have already registered for this webinar series please use the login information sent to you by webex.com.

For all webinars, CMS will make the slides available during or shortly after the presentation. CMS will advertise and update logistical information (dates/times, dial-in numbers, and webinar URLs) on the CMS zONE Private Issuer Community and Web-Broker Community webpage.

C. CMS zONE Communities (Guidance & Technical Resources)

CMS currently posts all technical information and guidelines, such as those referenced in this guidance, as well as webinar slide decks, assessment resources, and other documentation, on the CMS zONE DE Documents and Materials webpage at the following link: https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials.

This webpage is accessible by members of the Private Issuer Community (for issuers) and the CMS zONE Web-Broker Community (for web-brokers) only. CMS will post all webinar slide decks, and Frequently Asked Questions (FAQs) to these communities, and will highlight updates during the weekly ITWG webinars.

[33] Webinar Registration can be found at the following link on CMS zONE: https://zone.cms.gov/document/slides-cms-issuer-technical-workgroups-tuesdays

CMS will provide updates with further requirements and resources as they become available. A prospective web-broker should regularly check the DE Documents and Materials webpage. Unless otherwise specified, any guidance or requirements stated as forthcoming in this guidance are expected to be made available through the CMS zONE Communities for DE.

D. REGTAP

CMS will make DE resources available via REGTAP at the following link: https://www.regtap.info/.

E. Additional Guidance

- *Federally-facilitated Exchanges (FFEs) and Federally-facilitated Small Business Health Options Program (FF-SHOP) Enrollment Manual*: https://www.regtap.info/uploads/library/ENR_EnrollmentManualForFFEandFF-SHOP_v1_5CR_092519.pdf
- *Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements:* https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Guidelines-for-Third-Party-Auditors-EDE-PY20PY21-Year3.pdf
- Web-broker Guidance on CCIIO's Web-brokers in the Health Insurance Marketplace webpage: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Web-brokers-in-the-Health-Insurance-Marketplace.html
- *Frequently Asked Questions (FAQs) Regarding the* Quality Rating Information Bulletin's *(Quality Bulletin's) Display Guidelines for Direct Enrollment (DE) Entities Serving Consumers in States with Federally-facilitated Exchanges (FFEs) and State-based Exchanges on the Federal Platform (SBE-FPs)*: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/QRS-FAQs-for-DE-Entities.pdf
- For a current list of states that run their own State-based Exchange and do not use the federal platform, visit https://www.healthcare.gov/marketplace-in-your-state/. DE Entities can use this list with state website links to refer consumers or agents/brokers in these states to their state's website.
  - **Note:** Some states listed use the federal platform (HealthCare.gov) for individual coverage, but run their own FF-SHOP coverage operations. CMS will provide information to DE Entities if changes are made in the future.

Appendix A. Privacy and Security Controls for Web-brokers

The Web-Broker controls in Exhibit 4. 2020 Web-broker Agreement Security and Privacy Requirements Control Mapping are a streamlined subset of NEE SSP controls. For reference, Exhibit 4 maps all the controls (the main control and their enhancements) to the Web-Broker Agreement.

Please refer to the following statutory and regulatory provisions for the applicable federal privacy and security requirements: Patient Protection and Affordable Care Act ("PPACA") § 1312(e) and § 1411(g); 45 C.F.R. §§ 155.220, 155.221, 155.260, 155.280, and 155.1210.

Exhibit 4. 2020 Web-broker Agreement Security and Privacy Requirements Control Mapping

2020 Security and Privacy Requirements from the Web-broker Agreement	Web-broker Agreement Section	Applicable Security / Privacy Controls
1. Section 1312(e) of the PPACA provides that the Secretary of the U.S. Department of Health & Human Services ("HHS") shall establish procedures that permit Agents and Brokers to enroll Qualified Individuals in QHPs through an Exchange, and to assist individuals in applying for APTC and CSRs, to the extent allowed by States. To participate in the FFEs or SBE-FPs, including an FF-SHOP or SBE-FP SHOP, Agents, Brokers, and Web-brokers must complete all necessary registration and training requirements under 45 C.F.R. § 155.220.	WHEREAS: 1	N/A
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.	WHEREAS: 2	CA-3
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	WHEREAS: 3	CA-3

2020 Security and Privacy Requirements from the Web-broker Agreement	Web-broker Agreement Section	Applicable Security / Privacy Controls
PPACA and implementing regulations permit Web-broker to carry out. The Hub Web Services are not available for SHOP.		
4. Web-broker is an individual or entity licensed as an insurance producer, agent, or broker by the applicable state regulatory authority in at least one FFE or SBE-FP state; OR Web-broker is a Direct Enrollment Technology Provider.	WHEREAS: 4	N/A
5. Web-broker desires to gain access to the Hub Web Services, and to create, collect, disclose, access, maintain, store, and use PII from CMS, Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employers and Qualified Employees to perform the Authorized Functions described in Section II.a of this Agreement. The Hub Web Services are not available for SHOP.	WHEREAS: 5	CA-3
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 principles 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).	WHEREAS: 6	AR-7, CA-3
7. CMS has adopted privacy and security standards with which the Web-broker, a type of Non-Exchange Entity, must comply, which are set forth in Appendix A: Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities and the Non-Exchange Entity System Security and Privacy Plan.	WHEREAS: 7	PL-2
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 Appendix A: Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities and Appendix C: Standards for Communication with the Hub, as applicable, which are	II. Acceptance of Standard Rules of Conduct	PL-4

2020 Security and Privacy Requirements from the Web-broker Agreement	Web-broker Agreement Section	Applicable Security / Privacy Controls
incorporated by reference in this Agreement, while and as engaging in any activity as Web-broker for purposes of the PPACA. Web-broker shall strictly adhere to the privacy and security standards—and ensure that its employees, officers, directors, contractors, subcontractors, agents, and representatives strictly adhere to the same—to gain and maintain access to the Hub Web Services, if applicable, and to create, collect, disclose, access, maintain, store, and use PII for the efficient operation of the FFEs and SBE-FPs.		
a. Authorized Functions. Web-broker may create, collect, disclose, access, maintain, store, and use PII for: 1. Assisting with application, eligibility, and enrollment processes for QHP offered through the FFEs and SBE-FPs, including FF-SHOPs and SBE-FP-SHOPs; 2. Supporting QHP selection and enrollment by assisting with plan selection and plan comparisons; 3. Assisting with completing applications for the receipt of APTC or CSRs and with selecting an APTC amount, if applicable; 4. Facilitating the collection of standardized attestations acknowledging the receipt of the APTC or CSR determination, if applicable; 5. Assisting with the application for and determination of certificates of exemption, if applicable; 6. Assisting with filing appeals of eligibility determinations in connection with the FFEs and SBE-FPs, including Qualified Employer appeals for FF-SHOPs and SBE-FP-SHOPs; 7. Transmitting information about the Consumer's, Applicant's, Qualified Individual's, or Enrollee's decisions regarding QHP enrollment and/or CSR and APTC information to the FFEs and SBE-FPs, if applicable; 8. Facilitating payment of the initial premium amount to the appropriate individual market QHP, if applicable; 9. Facilitating payment of the initial and group premium amount for FF-SHOP and SBE-FP SHOP coverage, if applicable; 10. Facilitating an Enrollee's ability to disenroll from a QHP; 11. Educating Consumers, Applicants, or Enrollees on insurance affordability programs and, if applicable, informing such individuals of eligibility for Medicaid or Children's Health Insurance Program ("CHIP");	II. a. Authorized Functions.	DI-1, DI-1(1), DI-1(2), SI-10

2020 Security and Privacy Requirements from the Web-broker Agreement	Web-broker Agreement Section	Applicable Security / Privacy Controls
12. Assisting Enrollees to report changes in eligibility status to the FFEs and SBE-FPs throughout the coverage year, including changes that may affect eligibility (e.g., adding a dependent); 13. Handling FF-SHOP or SBE-FP SHOP coverage changes throughout the plan year that may impact eligibility, including, but not limited to, adding a new hire, removing an Employee no longer employed at the company, removing an Employee no longer employed full-time and adding a newborn or spouse during a special enrollment period, if applicable; 14. Correcting errors in the application for QHP enrollment; 15. Informing or reminding Enrollees when QHP coverage should be renewed, when Enrollees may no longer be eligible to maintain their current QHP coverage because of age, or to inform Enrollees of QHP coverage options at renewal; 16. Providing appropriate information, materials, and programs to Consumers, Applicants, Qualified Individuals, Enrollees, Employers, Employees, Qualified Employers, and Qualified Employees to inform and educate them about the use and management of their health information, as well as medical services and benefit options offered through the selected QHP or among the available QHP options; 17. Contacting Consumers, Applicants, Qualified Individuals, Enrollees, Employers, Employees, Qualified Employers and Qualified Employees to assess their satisfaction or resolve complaints with services provided by Web-broker in connection with the FFEs and SBE-FPs, including FF-SHOPs and SBE-FPSHOPs, 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		

2020 Security and Privacy Requirements from the Web-broker Agreement	Web-broker Agreement Section	Applicable Security / Privacy Controls
FF-SHOPs and SBE-FP-SHOPs, as permitted or required by Web-broker's contractual relationships with QHP Issuers; and 21. Performing other functions substantially similar to those enumerated above and such other functions that CMS may approve in writing from time to time.		
b. Standards Regarding PII. Web-broker agrees that it will create, collect, disclose, access, maintain, use, or store PII that it receives directly from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employers, and Qualified Employees, and from Hub Web Services, if applicable, only in accordance with all laws as applicable, including Section 1411(g) of the PPACA. The Hub Web Services are not available for SHOP.	II. b. Standards Regarding PII	AC-1, AC-2, AC-3, AC-6, AC-14, AC-17, AC-18, MP-1, MP-2, MP-4, MP-7, MP-7(1), MP, AP-1, AP-2, AR-1.

2020 Security and Privacy Requirements from the Web-broker Agreement	Web-broker Agreement Section	Applicable Security / Privacy Controls
1. Safeguards. Web-broker agrees to monitor, periodically assess, and update its security controls and related system risks to ensure the continued effectiveness of those controls in accordance with this Agreement, including Appendix A: Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities and the Non-Exchange Entity System Security and Privacy Plan. Furthermore, Web-broker agrees to timely inform the Exchange of any material change in its administrative, technical, or operational environments, or that would require an alteration of the privacy and security standards within this Agreement.	II. b. 1. Safeguards	AU-2, AU-2(3), AU-3, AU-4, AU-5, AU-5(1), AU-6, AU-8, AU-9, AU-11, AU-12, CA-1, CA-2, CA-2(1), CA-5, CA-6, CA-7, CM-2, CM-3, CM-8, CM-9, MA-5, MP-1, MP-5(4), PL-2, RA-1, RA-3, SA-4, SA-4(2), SA-9, SA-10, SI-4, SI-5, SI-12, SA-5, PE-1, PE-1, PE-3, PE-6, AR-4, AR-7
2. Downstream Entities. Web-broker will satisfy the requirement in 45 C.F.R. § 155.260(b) (2)(v) to bind downstream entities to the same privacy and security standards that apply to Non-Exchange Entities by entering into written agreements with any downstream entities that will have access to PII as defined in this Agreement. Web-broker must require in writing all downstream and delegated entities to adhere to the terms of this Agreement.	II. b. 2. Downstream Entities	PS-1, PS-6, PS-7
3. Critical Security and Privacy Controls. The critical controls the Web-broker must implement before Web-broker is able to submit any transactions to the FFE production system for individual market enrollments through the FFEs or SBE-FPs and/or assist Qualified Employers and Qualified Employees in purchasing and enrolling in coverage through an FF-SHOP or SBE-FP SHOP:	II. b. 3. Critical Security and Privacy Controls	(See below)
a. Email/Web Browser Protections – Including, but not limited to, assurance that transfer protocols are secure and limits the threat of communications being intercepted. Non-Exchange Entity SSP SC-7, AU-10, SC-1, SC-4, SC-8, SC-8(1), SC-8(2), SC13, SC-23, SC-28, and SC-CMS-1 controls.	II. b. 3. a. Email/Web Browser Protections	AU-10, SC-1, SC-4, SC-7, SC-8, SC-8(1), SC-8(2), SC-13, SC-23, SC-28, SC-CMS-1
b. Malware Protection – Including, but not limited to, protections against known threat vectors within the system's environment to mitigate damage/security breaches. Non-Exchange Entity SSP SI-1, SI-2, SI-3, SC-7, SC-1, and SC-CMS-1 controls.	II. b. 3. b. Malware Protection	SI-1, SI-2, SI-3, SI-3(2), SC-7, SC-1, SC-CMS-1
c. Patch Management – Including, but not limited to, ensuring every client and server is up to date with the latest security patches throughout the environment. Non-Exchange Entity SSP CM-1, CM-2, CM-3, CM-6, CM-8, CM-9, and CM-11 controls.	II. b. 3. c. Patch Management	CA-7, CM-1, CM-2, CM-3, CM-6, CM-8, CM-9, CM-11, RA-5, RA-5(1), RA-5(2), SI-5

2020 Security and Privacy Requirements from the Web-broker Agreement	Web-broker Agreement Section	Applicable Security / Privacy Controls
d. Vulnerability Management – Including, but not limited to, identifying, classifying, remediating, and mitigating vulnerabilities on a continual basis by conducting periodic vulnerability scans to identify weaknesses within an environment. Non-Exchange Entity SSP AU-2, AU-6, RA-3, RA-5, RA-5(1), RA-5(2), CA-7, and SI-5 controls.	II. b. 3. d. Vulnerability Management	AU-2, AU-6, CA-7, RA-3, RA-5, RA-5(1), RA-5(2), SI-5
e. Inventory of Software/Hardware – Including, but not limited to, maintaining an Inventory of hardware/software within the environment helps to identify vulnerable aspects left open to threat vectors without performing vulnerability scans and to have specific knowledge of what is within the system's environment. Non-Exchange Entity SSP AU-6, CM-8, SE-1, and PE-18 controls.	II. b. 3. e. Inventory of Software/Hardware	AU-6, CM-8, CM-8(1), CM-8(3), SE-1, PE-18
f. Account Management – Including, but not limited to, the determination of who/what has access to the system's environment and data and also maintain access controls to the system. Non-Exchange Entity SSP AC-1, AC-2, AC-3, AC-3(9), AC-6, AC-8, AC-14, AC-17, AC-18, AC-19, AC-20, AC-21, IA-1, IA-2, IA-2(1), IA- 2(2), IA-2(3), IA-2(8), IA-2(11), IA-3, IA-4, IA-5, IA-5(2), IA-5(3), IA-5(7), IA-5(11), IA-5(15), IA-5(1), IA-6, IA-7, IA-, PE-5, PE-4, PE-3, PS-4, and PS-5 controls.	II. b. 3. f. Account Management	AC-1, AC-2, AC-3, AC-3(9), AC-6, AC-8, AC-14, AC-17, AC-18, AC-19, AC-20, AC-21, IA-1, IA-2, IA-2(1), IA-2(2), IA-2(3), IA-2(8), IA-2(11), IA-3, IA-4, IA-5, IA-5(2), IA-5(3), IA-5(7), IA-5(11), IA-5(15), IA-5(1), IA-6, IA-7, IA-8, PE-1, PE-3, PE-4, PE-5, PE-6
g. Configuration Management – Including, but not limited to, defining the baseline configurations of the servers and endpoints of a system to mitigate threat factors that can be utilized to gain access to the system/data. Non-Exchange Entity SSP CM-1, CM-2, CM-3, CM-6, CM-8, CM-9, and CM-11 controls.	II. b. 3. g. Configuration Management	CM-1, CM-2, CM-3, CM-6, CM-8, CM-9, CM-11
h. Incident Response – Including, but not limited to, the ability to detect security events, investigate, and mitigate or limit the effects of those events. Non-Exchange Entity SSP AU-1, AU-2, AU-2(3), AU-3, AU-6, AU-9, AU-10, AU-11, AU-(12), AU- 12(1), IR-1, IR-2, IR-3, IR-3(2), IR-4, IR-4(1), IR-5, IR-6, IR-6(1), IR-7, IR-7(1), IR-8, IR-9, and CP-1 controls.	II. b. 3. h. Incident Response	AU-1, AU-2, AU-2(3), AU-3, AU-6, AU-9, AU-10, AU-11, AU-12, AU-12(1), IR-1, IR-2, IR-3, IR-3(2), IR-4, IR-4(1), IR-5, IR-6, IR-6(1), IR-7, IR-7(1), IR-8, IR-9, CP-1, SE-2
i. Governance and Privacy Compliance Program – Including, but not limited to, appointing a responsible official to develop and implement operational privacy compliance policies for information	II. b. 3. i. Governance and Privacy Compliance Program	AR-1, AR-4, AR-3

2020 Security and Privacy Requirements from the Web-broker Agreement	Web-broker Agreement Section	Applicable Security / Privacy Controls
systems and databases. Non-Exchange Entity SSP AR-1, AR-4, and AR-3 controls.		
j. Privacy Impact/Risk Assessment – Including, but not limited to, appointing a responsible official to develop and implement a formal policy and procedures to assess the organizations risk posture. Non-Exchange Entity SSP AR-2 controls.	II. b. 3. j. Privacy Impact/Risk Assessment	AR-2
k. Awareness and Training Program – Including, but not limited to, appointing a responsible official to develop and implement security and privacy education awareness program for all staff members and contractors. Non-Exchange Entity SSP AT-1, AT2, AT-2(2), and AT-4 controls.	II. b. 3. k. Awareness and Training Program	AT-1, AT-2, AT-2(2), AT-4
l. Data Retention and Destruction – Including, but not limited to, developing formal policy and procedures for data retention and destruction of PII. Non-Exchange Entity SSP AU-11, DM-2, DM-2(1), SI-12, MP-6, and AR-8 controls.	II. b. 3. l. Data Retention and Destruction	AU-11, DM-2, DM-2(1), SI-12, MP-6, AR-8
c. PII Received. Subject to the terms and conditions of this Agreement and applicable laws, in performing the tasks contemplated under this Agreement, Web-broker may create, collect, disclose, access, maintain, store, and use the following data and PII from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employers, and Qualified Employees including, but not limited to: (LIST)	II. c. PII Received	AR-1
d. Collection of PII. PII collected from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees and Qualified Employers—or their legal representatives or Authorized Representatives—in the context of completing an application for QHP, APTC, or CSR eligibility, if applicable, or enrolling in a QHP, or any data transmitted from or through the Hub, if applicable, may be used only for Authorized Functions specified in Section II.a of this Agreement. Such information may not be used for purposes other than authorized by this Agreement or as consented to by a Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee, and Qualified Employer.	II. d. Collection of PII	AP-1, AP-2, IP-1, MP-7, MP-7(1)
e. Collection and Use of Information Provided Under Other Authorities. This Agreement does not preclude Web-broker from collecting information from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees and Qualified Employers—or their legal representatives or Authorized Representatives—for a non-FFE/non-SBE-FP/non-Hub purpose, and using, reusing, and disclosing the non-FFE/non-SBE-FP/non-Hub information obtained as permitted by applicable law and/or other applicable authorities. Such information	II. e. Collection and Use of Information Provided Under Other Authorities	SC-7, SC-1, SC-4, AC-6, UL-1

2020 Security and Privacy Requirements from the Web-broker Agreement	Web-broker Agreement Section	Applicable Security / Privacy Controls
must be stored separately from any PII collected in accordance with Section II.c of this Agreement. The Hub Web Services are not available for SHOP.		
f. Ability of Individuals to Limit Collection and Use. Web-broker agrees to provide the Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee or Qualified Employer the opportunity to opt-in and have Web-broker collect, create, disclose, access, maintain, store and use their PII. Web-broker agrees to provide a mechanism through which the Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee and Qualified Employer can limit Web-broker's creation, collection, disclosure, access, maintenance, storage, and use of their PII to the sole purpose of obtaining Web-broker's assistance in applying for a QHP, APTC or CSR eligibility, if applicable, enrolling in a QHP offered through the FFEs or SBEFPs (including FF-SHOPs and SBE-FP-SHOPs), and for performing Authorized Functions specified in Section II.a of this Agreement.	II. f. Ability of Individuals to Limit Collection and Use	IP-1, IP-1(1), IP-3, IP-1, IP-4(1), UL-1, AC-6
g. Incident and Breach Reporting. Web-broker must implement Incident and Breach Handling procedures as required by the SSP and that are consistent with CMS's Incident and Breach notification Procedures. Such policies and procedures must identify the Web-broker's Designated Security and Privacy Official(s), if applicable, and/or identify other personnel authorized to access PII and responsible for reporting to CMS and managing Incidents or Breaches; provide details regarding the identification, response, recovery and follow-up of Incidents and Breaches, which should include information regarding the potential Non-Exchange Entity for CMS to immediately suspend or revoke access to the Hub for containment purposes; and require reporting of any security and privacy Incident or Breach of PII to the CMS IT Service Desk by telephone at (410) 786-2580 or 1-800-562-1963 or via email notification at cms_it_service_desk@cms.hhs.gov within one (1) hour after discovery of the Incident or Breach.	II. g. Incident and Breach Reporting	SE-2, IR-1, IR-2, IR-3, IR-3(2), IR-4, IR-4(1), IR-5, IR-6, IR-6(1), IR-7, IR-7(1) IR-8, IR-9, AU-6
d. Destruction of PII. Web-broker covenants and agrees to destroy all PII in its possession at the end of the record retention period required under Appendix A: Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities. If, upon the termination or expiration of this Agreement, Web-broker has in its possession PII for which no retention period is specified in Appendix A, such PII shall be destroyed within thirty (30) Days of the termination or expiration of this Agreement. Web-broker's duty to protect and maintain the privacy and security of PII, as provided for in Appendix A of this Agreement, shall continue in full force and effect	IV. Termination d. Destruction of PII	DM-1, DM-1(1), DM-2(1), MP-6, MP-6(1), MP-6(2), SI-12

2020 Security and Privacy Requirements from the Web-broker Agreement	Web-broker Agreement Section	Applicable Security / Privacy Controls
until such PII is destroyed and shall survive the termination or expiration of this Agreement.		
l. Audit and Compliance Review. Web-broker agrees that CMS, the Comptroller General, the Office of the Inspector General of HHS, or their designees may conduct compliance reviews or audits, which includes the right to interview employees, contractors and business partners of the Web-broker and to audit, inspect, evaluate, examine, and make excerpts, transcripts, and copies of any books, records, documents, and other evidence of Web-broker's compliance with the requirements of this Agreement upon reasonable notice to Web-broker, during Web-broker's regular business hours, and at Web-broker's regular business location. These audit and review rights include the right to audit Web-broker's compliance with and implementation of the privacy and security requirements under this Agreement. Web-broker further agrees to allow reasonable access to the information and facilities, including, but not limited to, Web-broker website testing environments, requested by CMS, the Comptroller General, the Office of the Inspector General of HHS, or their designees for the purpose of such a compliance review or audit. CMS may suspend or terminate this Agreement if a Web-broker does not comply with such a compliance review request within seven (7) Business Days. If any of Web-broker's obligations under this Agreement are delegated to other parties, the Web-broker's agreement with any delegated or downstream entities must incorporate this Agreement provision. This clause survives the expiration or termination of this Agreement.	V. Miscellaneous l. Audit and Compliance Review	CA-2, CA-2(1), CA-5, CA-7, SA-5
These standards and implementation specifications are established in accordance with Section 1411(g) of the Patient Protection and Affordable Care Act ("PPACA") (42 U.S.C. § 18081(g)), the Federal Information Management Act of 2014 ("FISMA") (44 U.S.C. § 3551), and 45 C.F.R. § 155.260. … The standards and implementation specifications that are set forth in this Appendix A are consistent with the principles in 45 C.F.R. § 155.260(a)(1) through (a)(6).	Appendix A: Statement of Applicability Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities	N/A

2020 Security and Privacy Requirements from the Web-broker Agreement	Web-broker Agreement Section	Applicable Security / Privacy Controls
(1) Individual Access to PII. In keeping with the standards and implementation specifications used by the FFEs, a Non Exchange Entity that maintains and/or stores PII must provide Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals' legal representatives and Authorized Representatives—with a simple and timely means of appropriately accessing PII pertaining to them and/or the person they represent in a physical or electronic readable form and format.	Appendix A: Non-Exchange Entity Privacy and Security Standards and Implementation Specifications (1) Individual Access to PII	IP-2, IP-3, IP-4, IP-4(1)
a. Standard: Individual Access to PII. A Non-Exchange Entity that maintains and/or stores PII must implement policies and procedures that provide access to PII upon request. The Non-Exchange Entity must comply with any additional standards and implementation specifications described in Non-Exchange Entity SSP IP-2: Individual Access.	Appendix A. (1) a. Standard: Individual Access to PII	IP-2
(2) Openness and Transparency. In keeping with the standards and implementation specifications used by the FFEs, a Non-Exchange Entity must ensure openness and transparency about policies, procedures, and technologies that directly affect Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers and their PII.	Appendix A. (2) Openness and Transparency	TR-1, TR-3
a. Standard: Privacy Notice Statement. Prior to collecting PII, the Non-Exchange Entity must provide a notice that is prominently and conspicuously displayed on a public-facing website, if applicable, or on the electronic and/or paper form the Non-Exchange Entity will use to gather and/or request PII. The Non-Exchange Entity must comply with any additional standards and implementation specifications described in Non-Exchange Entity SSP TR-1: Privacy Notice.	Appendix A. (2) a. Standard: Privacy Notice Statement	TR-1
4. If the Non-Exchange Entity operates a website, it shall ensure that descriptions of its privacy and security practices, and information on how to file complaints with CMS and the Non-Exchange Entity are publicly available through its website.	Appendix A. (2) a. i. Implementation Specifications. 4.	TR-1, TR-3, IP-4, IP-4(1)
(3) Individual Choice. In keeping with the standards and implementation specifications used by the FFEs, the Non-Exchange Entity should ensure that Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals' legal representatives or Authorized Representatives—are provided a reasonable	Appendix A. (3) Individual Choice	IP-1

2020 Security and Privacy Requirements from the Web-broker Agreement	Web-broker Agreement Section	Applicable Security / Privacy Controls
opportunity and capability to make informed decisions about the creation, collection, disclosure, access, maintenance, storage, and use of their PII.		
a. Standard: Informed Consent. The Non-Exchange Entity may create, collect, disclose, access, maintain, store, and use PII from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers —or these individuals' legal representatives or Authorized Representatives—only for the functions and purposes listed in the Privacy Notice Statement and any relevant agreements in effect as of the time the information is collected, unless the FFE, SBE-FP, FF-SHOP, FF-SBE SHOP, or Non-Exchange Entity obtains informed consent from such individuals. The Non-Exchange Entity must comply with any additional standards and implementation specifications described in Non-Exchange Entity SSP IP-1: Consent.	Appendix A. (3) a. Standard: Informed Consent	AP-2, IP-1, TR-1, UL-1
1. The Non-Exchange Entity must obtain informed consent from individuals for any use or disclosure of information that is not permissible within the scope of the Privacy Notice Statement and any relevant agreements that were in effect as of the time the PII was collected. Such consent must be subject to a right of revocation.	Appendix A. (3) (a) i. Implementation Specifications. 1.	IP-1, IP-1(1), TR-1
3. Consent documents must be appropriately secured and retained for ten (10) years.	Appendix A. (3) (a) i. Implementation Specifications. 3.	DM-2, DM-2(1), IP-1, SI-12
(4) Creation, Collection, Disclosure, Access, Maintenance, Storage, and Use Limitations. In keeping with the standards and implementation specifications used by the FFEs, the Non-Exchange Entity must ensure that PII is only created, collected, disclosed, accessed, maintained, stored, and used to the extent necessary to accomplish a specified purpose(s) in the contractual agreement and any appendices. Such information shall never be used to discriminate against a Consumer, Applicant, Qualified Individual, or Enrollee.	Appendix A. (4) (a). Creation, Collection, Disclosure, Access, Maintenance, Storage, and Use Limitations	AP-2, UL-1
a. Standard: Creation, Collection, Disclosure, Access, Maintenance, Storage, and Use Limitations. The Non-Exchange Entity must comply with the standards and implementation specifications described in Non-Exchange Entity SSP AP-1: Authority to Collect. Other than in accordance with the consent procedures outlined above, the Non-		TR-1, TR-3, CA-3, AP-1,

2020 Security and Privacy Requirements from the Web-broker Agreement	Web-broker Agreement Section	Applicable Security / Privacy Controls
Exchange Entity shall only create, collect, disclose, access, maintain, store, and use PII: i. In accordance with its published Privacy Notice Statement and any applicable agreements that were in effect at the time the PII was collected, including the consent procedures outlined above in Section (3); and/or ii. In accordance with the permissible functions outlined in the regulations and agreements between CMS and the Non-Exchange Entity		
b. Standard: Non-discrimination. Non-Exchange Entity should, to the greatest extent practicable, collect PII directly from the Consumer, Applicant, Qualified Individual, or Enrollee, when the information is likely to result in adverse determinations about benefits.	Appendix A. (4) (b): Standard: Non-discrimination	DI-1, SI-10
(5) Data Quality and Integrity. In keeping with the standards and implementation specifications used by the FFEs, Non-Exchange Entity should take reasonable steps to ensure that PII is complete, accurate, and up-to-date to the extent such data are necessary for Non-Exchange Entity's intended use of such data, and that such data have not been altered or destroyed in an unauthorized manner, thereby ensuring the confidentiality, integrity, and availability of PII. The Non-Exchange Entity must comply with any additional standards and implementation specifications described in Non-Exchange Entity SSP DI-1: Data Quality.	Appendix A. (5) Data Quality and Integrity	DI-1, DI-1(1), DI-1(2), SI-7, SI-7(1), SI-10
a. Standard: Right to Amend, Correct, Substitute, or Delete PII. In keeping with the standards and implementation specifications used by the FFEs, Non-Exchange Entity must offer Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers—or these individuals' legal representatives or Authorized Representatives—an opportunity and process to request amendment, correction, substitution, or deletion of PII maintained and/or stored by the Non-Exchange Entity if such individual believes that the PII is not accurate, timely, complete, relevant, or necessary to accomplish an Exchange-related function, except where the PII questioned originated from other sources, in which case the individual should contact the originating source. The Non-Exchange Entity must comply with any additional standards and implementation specifications described in Non-Exchange Entity SSP IP-3: Redress and IP-4: Complaint Management.	Appendix A. (5) (a) Standard: Right to Amend, Correct, Substitute, or Delete PII	IP-3, IP-4, IP-4(1)

2020 Security and Privacy Requirements from the Web-broker Agreement	Web-broker Agreement Section	Applicable Security / Privacy Controls
b. Standard: Verification of Identity for Requests to Amend, Correct, Substitute, or Delete PII. In keeping with the standards and implementation specifications used by the FFEs, a Non-Exchange Entity that maintains and/or stores PII must develop and implement policies and procedures to verify the identity of any person who requests access to, notification of, or modification—including amendment, correction, substitution, or deletion—of PII that is maintained by or for Non-Exchange Entity. This includes confirmation of an individual's legal or personal authority to access, receive notification of, or seek modification—including amendment, correction, substitution, or deletion—of a Consumer's, Applicant's, Qualified Individual's, or Enrollee's PII.	Appendix A. (5) (b) Standard: Verification of Identity for Requests to Amend, Correct, Substitute, or Delete PII	IP-3
c. Standard: Accounting for Disclosures. Except for those disclosures made to members of Non-Exchange Entity's Workforce who have a Non-Exchange Entity for the record in the performance of their duties, and the disclosures that are necessary to carry out the required functions of Non-Exchange Entity, a Non-Exchange Entity that maintains and/or stores PII shall maintain an accounting of any and all disclosures. The Non-Exchange Entity must comply with any additional standards and implementation specifications described in Non-Exchange Entity SSP AR-8: Accounting of Disclosures.	Appendix A. (5) (c) Standard: Accounting for Disclosures	AR-8, AU-2, AU-6
(6) Accountability. In keeping with the standards and implementation specifications used by the FFEs, a Non-Exchange Entity should adopt and implement the standards and implementation specifications in this document in a manner that ensures appropriate monitoring and other means and methods to identify and report Incidents and/or Breaches. The Non-Exchange Entity must comply with any additional standards and implementation specifications described in Non-Exchange Entity SSP SE-2 Privacy Incident Response.	Appendix A. (6) Accountability	AU-2, SE-2, IR-1, IR-2, IR-3, IR-3(2), IR-4, IR-4(1), IR-5, IR-6, IR-6(1), IR-7, IR-7(1), IR-8, IR-9
a. Standard: Reporting. The Non-Exchange Entity must implement Incident and Breach Handling Procedures that are consistent with CMS' Incident and Breach Notification Procedures and incorporate these procedures in the Non-Exchange Entity's own written policies and procedures.	Appendix A. (6) (a) Standard: Reporting	IR-1, IR-2, IR-3, IR-3(2), IR-4, IR-4(1), IR-5, IR-6, IR-6(1), IR-7, IR-7(1), IR-8, IR-9, SE-2

2020 Security and Privacy Requirements from the Web-broker Agreement	Web-broker Agreement Section	Applicable Security / Privacy Controls
b. Standard: Standard Operating Procedures. The Non-Exchange Entity shall incorporate privacy and security standards and implementation specifications, where appropriate, in its Standard operating procedures that are associated with functions involving the creation, collection, disclosure, access, maintenance, storage, or use of PII. The Non-Exchange Entity must comply with any additional standards and implementation specifications described in Non-Exchange Entity SSP AR-1: Governance and Privacy Program.	Appendix A. (6) (b) Standard: Standard Operating Procedures	AR-1, AC-2, AC-3, AC-14, AC-17, AC-17(3), MA-1, MA-5, MP-1, MP-2, MP-3, MP-4, MP-5, PS-2, PS-3, PS-8, DM-3, DM-3(1)
The Non-Exchange Entity shall complete an annual SPA assessment as described below. The SPA assessment shall include the following: • Documentation of existing security and privacy controls; • Identification of potential security and privacy risks; and • Corrective action plan describing approach and timeline to implement security and privacy controls to mitigate potential security and privacy risks.	Appendix A. Annual Security and Privacy Attestation (SPA)	CA-1, CA-2, CA-2(1), CA-5, PL-2, PL-4, RA-5
(1) Assessment Options. The following options are acceptable approaches for completing the SPA assessment: a. The Non-Exchange Entity may contract with a third party with experience conducting information system privacy and security audits to perform the SPA assessment. b. The Non-Exchange Entity may utilize internal information system staff resources to perform the SPA assessment, provided such staff have no direct responsibility for the security or privacy posture of the information system that is the subject of the SPA assessment. c. The Non-Exchange Entity may reference existing audit results that address some or all of the SPA assessment's requirements. Such existing audit results must have been generated using one of the methods described above in the first two assessment options. In addition, such existing audit results must have been produced within 365 days of completion of the SPA assessment. If existing audit reports do not address all required elements of the SPA assessment,	Appendix A. SPA (1) Assessment Options	CA-2(1), CA-2, PS-7

2020 Security and Privacy Requirements from the Web-broker Agreement	Web-broker Agreement Section	Applicable Security / Privacy Controls
the remaining elements must be addressed utilizing one of the first two assessment options.		
(2) Assessment Methodology. The SPA assessment methodology described herein is based on the standard CMS methodology used in the assessment of all CMS internal and business partner information systems. The Non-Exchange Entity shall prepare an assessment plan to evaluate any system vulnerabilities. The assessment methods may include examination of documentation, logs, and configurations; interviews of personnel; and/or testing of technical controls. The SPA assessment shall provide an accurate depiction of the security and privacy controls in place, as well as potential security and privacy risks, by identifying the following: a. Application or system vulnerabilities, the associated business and system risks and potential impact; b. Weaknesses in the configuration management process such as weak system configuration settings that may compromise the confidentiality, integrity, and availability of the system; c. Non-Exchange Entity security and privacy policies and procedures; and d. Major documentation omissions and/or discrepancies.	Appendix A. SPA (2) Assessment Methodology	CA-2, CA-5, PL-2, RA-3, RA-5
(3) Tests and Analysis Performed. The SPA assessment may include tests that analyze applications, systems, and associated infrastructure. The tests may begin with high-level analyses and increase in specificity. Tests and analyses performed during an assessment may include: a. Security control technical testing; b. Penetration testing; c. Adherence to privacy program policies; d. Network and component vulnerability scanning; e. Configuration assessment;	Appendix A. SPA (3) Tests and Analysis Performed	CA-2, CA-2(1), CA-8, AR-1, AR-2, RA-5, RA-5(1), RA-5(2), RA-5(5), CM-2, CM-6, CM-7, CM-9, SA-5

2020 Security and Privacy Requirements from the Web-broker Agreement	Web-broker Agreement Section	Applicable Security / Privacy Controls
f. Documentation review; g. Personnel interviews; and h. Observations.		
(4) Noncompliance and Applicability. The Non-Exchange Entity must develop a corrective action plan to mitigate any security and privacy risks if the SPA assessment identifies a deficiency in the Non-Exchange Entity's security and privacy controls. Alternatively, the Non-Exchange Entity may document why it believes a critical control is not applicable to its system or circumstances. The SPA assessment results do not alter the Agreement between the Non-Exchange Entity and CMS, including any penalties for non-compliance. If the Non-Exchange Entity's SPA assessment includes findings suggesting significant security or privacy risks, and the Non-Exchange Entity does not commence development and implementation of a corrective action plan to the reasonable satisfaction of CMS, a comprehensive audit may be initiated by CMS, and/or the Agreement between the Non-Exchange Entity and CMS may be terminated for cause.	Appendix A. SPA (4) Noncompliance and Applicability	CA-5
(5) Critical Security and Privacy Controls. The critical controls the Non-Exchange Entity must evaluate on an annual basis are: a. Email/Web Browser Protections – Including, but not limited to, assurance that transfer protocols are secure and limits the threat of communications being intercepted. Non-Exchange Entity SSP SC-7, AU-10, SC-1, SC-4, SC-8, SC-8(1), SC-8(2), SC-13, SC-23, SC-28, and SCCMS-1 controls. b. Malware Protection – Including, but not limited to, protections against known threat vectors within the system's environment to mitigate damage/security breaches. Non-Exchange Entity SSP SI-1, SI-2, SI-3, SC-7, SC-1, and SC-CMS-1 controls. c. Patch Management – Including, but not limited to, ensuring every client and server is up to date with the latest security patches throughout the environment. Non-Exchange Entity SSP CM-1, CM-2, CM-3, CM-6, CM-8, CM-9, and CM-11 controls. d. Vulnerability Management – Including, but not limited to, identifying, classifying, remediating, and mitigating vulnerabilities on a continual basis by conducting periodic vulnerability scans to identify	Appendix A. SPA (5) Critical Security and Privacy Controls	CA-2, CA-2(1), CA-7, and all controls listed above in section II. b. 3. Critical Security and Privacy Controls (see also below) a. SC-7, AU-10, SC-1, SC-4, SC-8, SC-8(1), SC-8(2), SC-13, SC-23, SC-28, SC-CMS-1 b. SI-1, SI-2, SI-3, SI-3(2), SC-7, SC-1, SC-CMS-1 c. CM-1, CM-2, CM-2(1), CM-3, CM-6, CM-8, CM-9, CM-11, RA-5, RA-5(1), RA-5(2), CA-7, SI-5

2020 Security and Privacy Requirements from the Web-broker Agreement	Web-broker Agreement Section	Applicable Security / Privacy Controls
weaknesses within an environment. Non-Exchange Entity SSP AU-2, AU6, RA-3, RA-5, RA-5(1), RA-5(2), CA-7, and SI-5 controls. e. Inventory of Software/Hardware – Including, but not limited to, maintaining an Inventory of hardware/software within the environment helps to identify vulnerable aspects left open to threat vectors without performing vulnerability scans and to have specific knowledge of what is within the system's environment. Non-Exchange Entity SSP AU-6, CM-8, SE-1, and PE-18 controls. f. Account Management —Including, but not limited to, the determination of who/what has access to the system's environment and data and also maintain access controls to the system. Non-Exchange Entity SSP AC-1, AC-2, AC-3, AC-6, AC-8, AC-14, AC-17, AC-18, AC-19, AC-20, AC-21, IA-1, IA-2, IA-2(1), IA-2(2), IA-2(3), IA-2(8), IA-2(11), IA-3, IA-4, IA-5, IA-5(2), IA-5(3), IA-5(7), IA-5(11), IA-5(15), IA-5(1), IA-6, IA-7, IA-8, PE5, PE-4, PE-3, PS-4, and PS-5 controls. g. Configuration Management – Including, but not limited to, defining the baseline configurations of the servers and endpoints of a system to mitigate threat factors that can be utilized to gain access to the system/data. Non-Exchange Entity SSP CM-1, CM-2, CM-3, CM-6, CM-8, CM-9, and CM-11 controls. h. Incident Response – Including, but not limited to, the ability to detect security events, investigate, and mitigate or limit the effects of those events. Non-Exchange Entity SSP AU-1, AU-2, AU-2(3), AU-3, AU-6, AU-9, AU-10, AU-11, AU-(12), AU-12(1), IR-1, IR-2, IR-3, IR-3(2), IR-4, IR-4(1), IR-5, IR-6, IR-6(1), IR-7, IR-7(1), IR-8, IR-9, and CP-1 controls. i. Governance and Privacy Compliance Program – Including, but not limited to, appointing a responsible official to develop and implement operational privacy compliance policies for information systems and databases. Non-Exchange Entity SSP AR-1, AR-3, and AR-4 controls. j. Privacy Impact/Risk Assessment – Including, but not limited to, appointing a responsible official to develop and implement a formal policy and procedures to assess the organizations risk posture. Non-Exchange Entity SSP AR-2 control.		d. AU-2, AU-6, RA-3, RA-5, RA-5(1), RA-5(2), CA-7, SI-5 e. CM-8, CM-8(1), CM-8(3) f. AC-1, AC-2, AC-3, AC-6, AC-8, AC-14, AC-17, AC-18, AC-19, AC-20, AC-21, PE-1, PE-3, PE-4, PE-5, PE-6 IA-1, IA-2, IA-2(1), IA-2(2), IA-2(3), IA-2(8), IA-2(11), IA-3, IA-4, IA-5, IA-5(2), IA-5(3), IA-5(7), IA-5(11), IA-5(15), IA-5(1), IA-6, IA-7, IA-8 g. CM-1, CM-2, CM-3, CM-6, CM-8, CM-9, and CM-11. h. AU-1, AU-2, AU-2(3), AU-3, AU-6, AU-9, AU-10, AU-11, AU-12, AU-12(1), IR-1, IR-2, IR-3, IR-3(2), IR-4, IR-4(1), IR-5, IR-6, IR-6(1), IR-7, IR-7(1), IR-8, IR-9, CP-1, SE-2 i. AR-1, AR-3, AR-4 j. AR-2 k. AT-1, AT-2, AT-2(2), AT-4

2020 Security and Privacy Requirements from the Web-broker Agreement	Web-broker Agreement Section	Applicable Security / Privacy Controls
k. Awareness and Training Program – Including, but not limited to, appointing a responsible official to develop and implement security and privacy education awareness program for all staff members and contractors. Non-Exchange Entity SSP AT-1, AT-2, AT-2(2), and AT-4 controls. l. Data Retention and Destruction – Including, but not limited to, developing formal policy and procedures for data retention and destruction of PII. Non-Exchange Entity SSP AU-11, DM-2, DM-2(1), SI-12, MP-6, AR-8 controls.		l. AU-11, DM-2, DM-2(1), SI-12, MP-6, AR-8
(6) Non-Exchange Entity System Security Plan (“SSP”) which is based on NIST National Institute for Standards and Technology Special Publication 800-53, Revision 4. Independent third-party auditor verification and documentation of the Non-Exchange Entity’s compliance with some or all of Non-Exchange Entity controls that correspond to the critical controls listed above shall be accepted by CMS as documentation of compliance with those critical controls.	Appendix A. SPA (6) Non-Exchange Entity System Security Plan (“SSP”) which is based on NIST National Institute for Standards and Technology Special Publication 800-53, Revision 4.	CA-2(1), PL-2
(9) CMS Verification of SPA. CMS will review the Non-Exchange Entity’s SPA assessment, and for any critical security or privacy control that the Non-Exchange Entity claimed as not applicable, CMS, in its sole discretion, will determine if the claim is justified. If CMS determines such controls are applicable, CMS may require a supplementary assessment of such controls and an amended SPA submission from the Non-Exchange Entity. If the SPA assessment indicates that the Non-Exchange Entity does not meet any critical control, CMS may require remedial action. A Non-Exchange Entity that does not complete a SPA assessment or any required supplemental assessment or remedial actions may be subject to the Termination with Cause provision (Section IV, b) of this Agreement.	Appendix A. SPA (9) CMS Verification of SPA	CA-2, CA-2 (1), CA-5