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

Date: January 10, 2024
From: Center for Consumer Information and Insurance Oversight (CCIIO)
Title: Health Insurance Exchange Guidelines
Subject: Web-broker Operational Readiness Reviews for the Classic Direct Enrollment and Enhanced Direct Enrollment Pathways and Related Oversight Requirements

Contents

I. Background

These guidelines, which update the May 21, 2020 guidance entitled *Updated Web-broker Direct Enrollment Program Participation Minimum Requirements for plan year (PY) 2022,* describes minimum requirements for web-brokers[1] participating in or seeking approval to participate in the Direct Enrollment (DE) program in states with Exchanges that use the Federal Platform, including Federally-facilitated Exchanges (FFEs) and State-based Exchanges on the Federal

[1] See Section II of these guidelines for the definition of a "web-broker."

Platform (SBE-FPs) (collectively referred to as the Exchanges, and individually referred to as an Exchange). The guidelines are applicable to web-brokers that are approved to use—and prospective web-brokers that seek approval to use—the classic DE and/or enhanced direct enrollment (EDE) pathways to assist consumers with direct enrollment in coverage in a manner that constitutes enrollment in an Exchange or assisting individual market consumers with submission of applications for advance payments of the premium tax credit and cost-sharing reductions to an Exchange.[2]

These web-broker operational readiness requirements apply to web-brokers regardless of the DE pathway that the web-broker uses. Throughout these guidelines, references to "DE," without specifying either classic DE or EDE, are inclusive of both the classic DE and EDE pathways.

These guidelines provide details on the minimum requirements for web-brokers participating in and seeking approval to participate in the DE program.[3] As discussed in the following sections, before web-brokers can allow consumers to use their internet website to complete an Exchange eligibility application or a qualified health plan (QHP)[4] selection, web-brokers must demonstrate compliance with applicable business requirements set forth 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)[5] and submit privacy and security-related documentation demonstrating that they have complied with privacy and security requirements in the Web-broker Agreement and applicable federal privacy and security regulations.[6]

Web-brokers using or seeking to use the EDE pathway must also comply with additional requirements that are set forth in CCIIO's annual Enhanced Direct Enrollment (EDE) Guidelines entitled *Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements*.[7] Note that satisfying some of the EDE-specific

---

[2] The classic DE and EDE pathways include both the consumer-facing and agent/broker-facing pathways. Consumer-facing pathway means the workflow, UI, and accompanying APIs for a DE environment that is intended for use by a Consumer to complete an eligibility application and enrollment. Agent/broker-facing pathway means the workflow, UI, and accompanying APIs for a DE environment that is intended for use by an agent/broker to assist a consumer with completing an eligibility application and enrollment.

[3] See 45 C.F.R. §§ 155.220(c)(6) and 155.221(b)(4).

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

[5] The Web-broker Agreement for the current plan year is available at the following link on CMS zONE: https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials. CMS approval to access the Web-broker Community on CMS zONE is required to access CMS zONE links referenced in these guidelines.

[6] See 45 C.F.R. § 155.220(c)(6) and (d); 45 C.F.R. § 155.221(b)(4), (b)(5), and (f); and 45 C.F.R. § 155.260(b).

[7] See 45 C.F.R. § 155.221(f) and (g)(2). The requirements to operate as an EDE Entity are detailed in the Guidelines for Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements (the EDE Guidelines) for the current year, which are available at the following link under the header "Enhanced Direct Enrollment Resources (Issuers and Web-brokers): https://www.cms.gov/programs-and-initiatives/health-insurance-marketplaces/direct-enrollment-and-enhanced-direct-enrollment. CMS expects to update the EDE Guidelines on an annual basis prior to the annual EDE audit submission window. Prospective and existing EDE Entities should verify they are reviewing the most recent EDE Guidelines. The EDE Guidelines for Year 6 (published March 1, 2023) are available at the following link: https://www.cms.gov/files/document/guidelines-enhanced-direct-enrollment-audits-year-6-final.pdf. On March 8, 2022, CMS published *Frequently Asked Questions (FAQs) Regarding the Audit Submission Timeline for Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment (EDE) Pathway for Calendar Year*

requirements contained therein may constitute satisfaction of some of the requirements described in these guidelines.[8]

If, after thoroughly reviewing the requirements in this document, an entity would like to be considered for approval to operate as a web-broker on the Exchanges, please contact directenrollment@cms.hhs.gov. Please note, web-brokers *must* develop their own technical environment and integrate with the CMS-provided DE APIs[9] in order to offer a DE environment[10] for use by Exchange consumers, agents, and brokers. CMS does not provide agents, brokers, or prospective web-brokers with an existing DE environment that will allow agents, brokers, and consumers to enroll consumers in QHP coverage or complete an Exchange eligibility application. Agents and brokers interested in using an existing, but not developing a new, DE environment should review the list of approved web-brokers and approved EDE entities to identify a DE environment and DE entity to contact about using their non-Exchange website to assist consumers.[11]

A. Authority

Pursuant to 45 C.F.R. §§ 155.220(c)(6) and 155.221(b)(4), web-brokers must demonstrate operational readiness and compliance with applicable requirements prior to their websites being used to complete an Exchange eligibility application or a QHP selection.

During the web-broker onboarding process, CMS will review a prospective web-broker's website for compliance with applicable requirements, including 45 C.F.R. § 155.220(c)(3) and (j).[12]

A web-broker must oversee the downstream agents or brokers using its DE environment consistent with 45 C.F.R. § 155.220(c)(4). This includes a requirement to verify that agents and brokers using the web-broker's non-Exchange website are appropriately licensed in the State in which the consumer is selecting a QHP and have completed training and registration—including signing the required agreements—with the Exchange, pursuant to 45 CFR 155.220(c)(4)(i)(B). Pursuant to 45 C.F.R. § 155.220(c)(4)(ii), CMS may temporarily suspend a web-broker's ability to transact information with HHS if CMS discovers a security and privacy incident or breach, for

---

2022 and Subsequent Calendar Years, clarifying the time frame for the annual audit submission window, available at the following link: https://www.cms.gov/files/document/2022-and-subsequent-calendar-years-ede-audit-submission-timeline-faqs.pdf.

[8] See, e.g., Section VI of these guidelines for specific information on how web-brokers approved to use or seeking to be approved to use the EDE pathway may satisfy the web-broker operational readiness requirements by satisfying EDE pathway program requirements.

[9] For more information on how to integration with CMS DE APIs, see Exhibit 3: Web-broker Onboarding Process.

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

[11] The list of approved Web-brokers and entities approved to use EDE are available at the following link: https://www.cms.gov/programs-and-initiatives/health-insurance-marketplaces/direct-enrollment-and-enhanced-direct-enrollment.

[12] See 45 C.F.R. § 155.220(c)(6)(iii).

the period in which HHS begins to conduct an investigation and until the incident or breach is remedied to CMS's satisfaction. In addition, pursuant to 45 C.F.R. § 155.220(k)(3), CMS may immediately suspend a web-broker's ability to transact information with HHS if CMS discovers circumstances that pose unacceptable risk to Exchange operations or Exchange information technology systems until the incident or breach is remedied or sufficiently mitigated to CMS' satisfaction.

CMS may suspend or terminate a web-broker's agreement(s) with the Exchange or deny the web-broker the right to enter into agreements with the Exchange in future years under 45 C.F.R. §§ 155.220(g) and (m), respectively, for the failure to comply with applicable requirements. Additionally, 45 C.F.R. § 155.220(k) describes penalties other than termination of a web-broker's agreement(s) with the Exchange that CMS may impose on a web-broker for failure to comply with the requirements of 45 C.F.R. § 155.220.

Pursuant to 45 C.F.R. § 155.220(l), if a web-broker enrolls qualified individuals, qualified employers, or qualified employees in coverage in a manner that constitutes enrollment through an SBE-FP or assists individual market consumers with submission of applications for advance payments of the premium tax credit and cost-sharing reductions through an SBE-FP, the web-broker must comply with all applicable FFE standards in 45 C.F.R. § 155.220. Web-brokers must also comply with the privacy and security standards set forth in the Web-broker Agreement and the *Non-Exchange Entity System Security and Privacy Plan* (NEE SSP).[13,14]

These guidelines do not supersede EDE program requirements for web-brokers that are EDE Entities. Web-brokers that seek to become or that CMS has approved to operate as an EDE Entity must comply with all web-broker requirements and EDE program requirements.[15] CMS also conducts ongoing oversight of web-brokers, once approved, including regular reviews of web-brokers' websites for compliance with the website display requirements detailed in 45 C.F.R. §§ 155.220(c)(3)and 155.221 (b)(1)-(3) and (c), the Web-broker Agreement, and program guidance.[16]

II. Web-broker Overview

Web-broker is defined in 45 C.F.R. § 155.20 and refers to an individual agent, broker, group of agents or brokers, or business entity registered with an Exchange under § 155.220(d)(1) that develops and hosts a non-Exchange website that interfaces with an Exchange to assist consumers with direct enrollment in QHPs offered through the Exchange as described in § 155.220(c)(3) or § 155.221. The term web-broker is inclusive of agent or broker DE technology providers (DE TPs). An agent or broker DE technology provider (as defined in 45 C.F.R. § 155.20) is a type of web-broker business entity that is not a licensed agent or broker under State law and has been

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

[14] Web-brokers are a non-Exchange entity, as that term is defined in 45 C.F.R. § 155.260(b)(1).

[15] The requirements to operate as an EDE Entity are detailed in the EDE Guidelines for the current year, which are available at the following link under the header "Enhanced Direct Enrollment Resources (Issuers and Web-brokers)": https://www.cms.gov/programs-and-initiatives/health-insurance-marketplaces/direct-enrollment-and-enhanced-direct-enrollment.

[16] CMS posts relevant program guidance for web-brokers on CMS zONE in the Web-broker Community (available at: https://zone.cms.gov/community/web-broker-community) and on the Direct Enrollment and Enhanced Direct Enrollment Resources webpage (available at: https://www.cms.gov/marketplace/agents-brokers/direct-enrollment-partners).

engaged or created by, or is owned by an agent or broker, to provide technology services (i.e., a DE environment) to facilitate participation in direct enrollment under §§ 155.220(c)(3) and 155.221.. Web-brokers are one defined entity type within the category of DE Entities.[17] Web-brokers, unlike QHP issuers that participate in DE, must provide a QHP shopping experience that displays all QHPs available in a service area with the required QHP comparative information for consumers, agents, and brokers.[18]

This section will further describe the permissible arrangements through which a web-broker can provide the use of a DE environment to end users (i.e., agents, brokers, and consumers). All arrangements must be operated in compliance with applicable state and federal laws and regulations, including 45 C.F.R. §§ 155.220, 155.221, 155.260(b), and 156.1230.

A. Classic Direct Enrollment and Enhanced Direct Enrollment Definitions

Web-brokers may host a classic DE and/or an EDE environment capable of assisting consumers with completing an Exchange[19] eligibility application and enrolling in QHPs offered through the Exchange. For the classic DE pathway, the consumer or agent/broker is redirected to HealthCare.gov to complete the eligibility application and redirected back to the web-broker's classic DE non-Exchange website to complete enrollment. The EDE pathway allows approved EDE Entities to host an eligibility application for Exchange coverage on an EDE Entity's website and does not require the consumer or agent/broker to be redirected to HealthCare.gov for that portion of the application and enrollment process.

Web-broker websites can be used directly by consumers (i.e., consumer-facing websites) or agents and brokers (i.e., agent/broker-facing websites). A consumer-facing DE web-broker website allows a consumer—either working independently or with an agent/broker—to submit an Exchange eligibility application and complete the QHP selection. An agent/broker-facing DE web-broker website is utilized by agents and brokers to assist the consumer with the completion of the Exchange eligibility application and QHP selection. While these types of websites differ in some ways, both are subject to requirements in 45 C.F.R. §§ 155.220 and 155.221.

B. Web-broker Required Arrangements with Agents and Brokers

CMS requires web-brokers to work in connection with a licensed agent or broker to assist consumers with enrolling in QHPs through the Exchanges. This arrangement may come in many forms, but a web-broker must comply with state law regarding licensure and appointment in each state in which a web-broker operates. For example, subject to applicable state law, a web-broker may operate as a licensed agency or brokerage business entity or as an agent or broker DE technology provider that provides a DE environment to one or more licensed agents or brokers.

---

[17] Direct enrollment entities(DE Entities) can include web-brokers, QHP issuers, and QHP Issuer and Agent or Broker DE Technology Providers (defined in 45 C.F.R. § 155.20). DE Entities are entities that an Exchange permits to assist consumers with direct enrollment in QHPs offered through the Exchange in a manner considered to be through the Exchange as authorized by § 155.220(c)(3), § 155.221, or § 156.1230. See § 155.20. These guidelines, however, are only applicable to DE Entities that are web-brokers and Agent or Broker DE Technology Providers.

[18] CMS publishes Web-broker website display guidance in the *Key Resources* section of the Direct Enrollment/Enhanced Direct Enrollment Resources for the Federally-facilitated Exchange webpage, available at the following link: https://www.cms.gov/programs-and-initiatives/health-insurance-marketplaces/direct-enrollment-and-enhanced-direct-enrollment.

[19] Exchange has the meaning set forth in 45 C.F.R. § 155.20.

An agent or broker DE technology provider cannot provide a DE environment directly to consumers for completing an Exchange eligibility application and enrolling in a QHP (i.e., they must provide the environment on behalf of a licensed agent/broker for use by consumers) because they are not a licensed agent or broker under state law.[20]

Pursuant to 45 C.F.R. §§ 155.220(c)(4), web-brokers must oversee the agents and brokers that the web-broker allows to use its DE environment for compliance with CMS regulatory requirements and state licensure requirements.

C. Web-broker DE Services Provided Directly to End-Users

Web-brokers can offer the use of a DE environment directly to end users (i.e., consumers, agents, and brokers) subject to the requirements described in Section II.B of these guidelines. For example, web-brokers can provide a public-facing website to consumers or websites designed for use by agents and brokers that have contracted with the web-broker. Furthermore, web-brokers can provide public-facing websites for agents and brokers that are controlled by the web-broker, but labeled with the agent's or broker's branding and marketing information for use by consumers (i.e., "white-label" arrangements). All web-broker websites that facilitate completion of an Exchange eligibility application or QHP enrollment through an Exchange must comply with the requirements in 45 C.F.R. §§ 155.220 and 155.221, including the requirement to display all QHPs and required QHP comparative information. Except as provided in Section II.D of these guidelines, the QHP display used to select a QHP for enrollment via a DE environment must be provided and controlled by the web-broker. The web-broker must not allow or facilitate the use of QHP selections outside of the QHP display provided and controlled by the web-broker in these types of arrangements.[21]

D. Web-broker DE Environment Use by Other CMS-approved Entities and Indirectly to End Users

Web-brokers can offer the use of their DE Environment indirectly to end users on behalf of another CMS-approved DE entity (i.e., QHP issuers, web-brokers, or hybrid non-issuer upstream EDE Entities).[22]

Web-brokers can provide DE environments on behalf of QHP issuers by operating as a qualified health plan issuer direct enrollment technology provider (as defined in 45 C.F.R. § 155.20). These DE environments can be used by consumers to complete an Exchange eligibility application and enroll in the QHP issuer's QHPs offered through an Exchange, and by agents or brokers to assist consumers in doing the same. In this arrangement, the web-broker operating as a QHP issuer DE technology provider would be a downstream and delegated entity of the QHP issuer subject to the requirements set forth in 45 C.F.R. § 156.340. The web-broker operating as a QHP issuer DE technology provider must comply with all applicable Federal standards related

[20] All references to agents and brokers in these guidelines refer to agents and brokers that are licensed in the applicable state and have completed the annual FFE registration and training.

[21] For a limited exception to this rule, please refer to Section II.D.

[22] Hybrid non-issuer upstream EDE Entities are a type of upstream EDE Entity. As described in the EDE Guidelines for Year 6 in Section IV.A.iii, a hybrid non-issuer upstream EDE Entity is an agent, broker, or web-broker that uses a primary EDE Entity's EDE environment with additional functionality or systems that modify the EDE end-user experience provided by the primary EDE Entity. The EDE Guidelines for Year 6 are available at the following link: https://www.cms.gov/files/document/guidelines-enhanced-direct-enrollment-audits-year-6-final.pdf.

to Exchanges, including those detailed in 45 C.F.R. §§ 155.221 and 156.1230. The web-broker operating as the QHP issuer's DE technology provider must use the issuer's Hub partner ID for DE enrollment activity conducted on behalf of the issuer. Furthermore, a web-broker in this relationship can provide consumer-facing, white-label websites through the DE environment for both consumers and agents and brokers to assist consumers with submitting Exchange eligibility applications and enrolling in the QHP issuer's plans offered on the Exchange. In these arrangements with QHP issuers, web-brokers *may* allow the use of QHP selections completed on QHP issuer-provided, -controlled, and -owned QHP selection websites. For example, a QHP issuer provides a QHP selection of its own plans on its own website, which redirects the end user to the web-broker's website to complete the Exchange eligibility application and QHP enrollment process. However, this permissibility does not extend to agent- or broker-owned, controlled websites providing a QHP display on behalf of the issuer.

Web-brokers can also provide their DE environments to other web-brokers or hybrid non-issuer upstream EDE Entities. In these scenarios, the QHP display used to select a QHP for enrollment via a DE environment must be provided and controlled by the web-broker. The web-broker that provides the DE environment must not allow or facilitate the use of QHP selections made outside of the QHP display provided and controlled by a web-broker for enrollment via classic DE or EDE.

E. Differences Between QHP Issuer DE Technology Providers and Web-brokers

As noted above, a web-broker may operate as a QHP issuer DE technology provider and provide DE services to a QHP issuer. However, a QHP issuer DE technology provider cannot operate as a web-broker or provide web-broker-like services (as described in Section II of these guidelines) without becoming a web-broker. This section details the distinctions between QHP issuer DE technology providers and web-brokers.

Entities that operate only as a QHP issuer DE technology provider may only provide a DE environment to QHP issuers, and, on behalf of that issuer, to the issuer's downstream users (i.e., consumers, agents, and brokers). In this capacity, QHP issuer DE technology providers can provide classic DE environments or EDE environments.

However, unlike web-brokers, QHP issuer DE technology providers cannot display plans or provide a DE environment directly to consumers or agents and brokers independent of an arrangement with a specific QHP issuer. The ability of a QHP issuer DE technology provider to display QHPs and facilitate enrollment in those QHPs is dependent on a connection to an agent, broker, or QHP issuer, consistent with state law. Accordingly, in order to do so, a QHP issuer DE technology provider would need to onboard as a web-broker with CMS and comply with the requirements described in Section II.B of these guidelines (i.e., a web-broker's required arrangements with agents and brokers).

If a QHP issuer DE technology provider seeks to provide an EDE environment directly to consumers, agents, and brokers—that is, not on behalf of a QHP issuer—a QHP issuer DE technology provider can become a web-broker by completing the web-broker onboarding process, as described in Sections III and IV. Due to the different operating models of QHP issuer DE technology providers and web-brokers, the QHP issuer DE technology provider may need to modify its EDE environment to comply with the requirements applicable to web-brokers (e.g.,

the requirement to display all available QHPs offered on the Exchange, rather than just display the QHP issuer's plans offered on the Exchange). The QHP issuer DE technology provider must make such changes prior to conducting the privacy and security audit and before CMS will conduct a pre-approval website review as part of the web-broker onboarding process.

If CMS has approved the QHP issuer DE technology provider to operate as a primary EDE Entity, the QHP issuer DE technology provider may be able to satisfy some of the web-broker operational readiness requirements leveraging its approval as a primary EDE Entity, as described in Section VI.B.i.[23]

If a QHP issuer DE technology provider has not been approved as a primary EDE Entity or is only seeking approval to operate as a classic DE web-broker, the QHP issuer DE technology provider should progress through the full web-broker onboarding process as described in Section IV.

III. Web-broker Operational Readiness Review Requirements

CMS has established operational readiness review requirements that web-brokers must meet and demonstrate compliance with CMS prior to approval and, at a minimum, on an annual basis thereafter. These requirements and CMS' approval of web-brokers are necessary because of the effects a web-broker's processes may have on the HealthCare.gov information technology (IT) platform and consumers' Exchange eligibility applications and enrollments in QHPs offered through the Exchange. A prospective web-broker must satisfy the web-broker operational readiness review requirements before CMS will countersign the prospective web-broker's Web-broker Agreement and enable the web-broker's access to the production DE environments. An existing web-broker must similarly satisfy the applicable operational readiness review requirements on an annual basis to maintain CMS' approval to operate a classic DE or EDE environment.[24] This section details the operational readiness review requirements for web-brokers to obtain and maintain CMS' approval to operate a classic DE or EDE environment in production.

A. Web-broker Privacy and Security Requirements

i. Web-broker Privacy and Security Audit Requirements

Web-brokers must implement the privacy and security controls[25] set forth in the NEE SSP and consistent with the requirements in the Web-broker Agreement (see, e.g., Sections III, V, and IX

[23] A primary EDE Entity, as described in Section IV.A of the EDE Guidelines for Year 6, is an entity that develops, designs, and hosts its own EDE environment for its own use or for use by others. A primary EDE Entity must undergo both the third-party privacy and security and business audits prior to CMS approving the primary EDE Entity's EDE environment. The EDE Guidelines for Year 6 are available at the following link: https://www.cms.gov/files/document/guidelines-enhanced-direct-enrollment-audits-year-6-final.pdf.

[24] For more information on the applicable operational readiness review requirements that existing web-brokers must satisfy on an annual basis, review Section IV.B of these guidelines. Note: These operational readiness review requirements are independent of the EDE operational readiness review requirements–as defined in the EDE Guidelines–unless otherwise noted.

[25] As detailed in Section VI of these guidelines, additional privacy and security controls apply to web-brokers participating in EDE.

of the Web-broker Agreement for plan year 2024) to participate in classic DE.[26] The NEE SSP contains comprehensive security and privacy controls and implementation standards for all aspects of the DE program. Beyond the required controls for the web-broker operational readiness review requirements for privacy and security, CMS strongly recommends web-brokers participating in classic DE implement all of the NEE SSP controls. The NEE SSP describes the annual assessment that web-brokers must conduct, including the assessment methodology, and the tests and analysis to be performed on an annual basis. This privacy and security audit must be conducted by one or more independent, objective third-party auditors free of any real or perceived conflict(s) of interest, consistent with 45 C.F.R. § 155.221(f), (g), and (h) and Section IX of the Web-broker Agreement."

For an existing web-broker, the web-broker must complete an annual privacy and security audit consistent with the Non-Exchange Entity (NEE) Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide and the NEE SSP.[27]

For a prospective web-broker, the privacy and security audit must be conducted after the web-broker has completed development of its DE environment. The DE environment subject to the audit must represent the DE environment that the web-broker intends to use in production to connect to the Exchange.

To demonstrate compliance with the requirements in Appendix A of the Web-broker Agreement, web-brokers are required to submit the complete set of documents outlined in Exhibit 1 to CMS, unless otherwise noted in the "Submission Requirements" column.[28] All assessment activities that serve as the basis for the documentation in Exhibit 1 must have been completed within one year of the date of the fully executed Web-broker Agreement (i.e., the date of the relevant Security and Privacy Assessment Report (SAR) the web-broker is using to satisfy the annual privacy and security requirements required by these guidelines must be within one year of the date that CMS provides the web-broker an executed Web-broker Agreement).

Exhibit 1: Required Privacy and Security Documentation for Web-broker Annual Assessment

Document	Description	Submission Requirements
Security Privacy Controls Assessment	▪ The SAP describes the auditor's scope and methodology of the assessment. ▪ The SAP includes an attestation of the auditor's independence.	▪ Submit via the Entity-specific DE/EDE PME site at least thirty (30) days before commending the privacy and security audit during the planning phase.[29]

[26] The NEE SSP is available on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit.

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

[28] 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(g)(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 7 and Section VI of these guidelines for more information.

[29] For more information on requesting access to an Entity-specific DE/EDE PME site, please review Section VIII.

Document	Description	Submission Requirements
Test Plan (SAP)	▪ The SAP must be completed by the auditor and submitted to CMS for review, prior to conducting the security and privacy controls assessment (SCA).	▪ After CMS has received the SAP and auditor contract, CMS will schedule an audit kick-off call with the prospective web-broker and auditor. ▪ For any existing web-brokers, consistent with the ISCM Strategy Guide, this step is only required if the web-broker is changing auditors for its annual assessment.
Auditor Contract	▪ The prospective web-broker must submit a contract with its selected privacy and security auditor. ▪ The prospective web-broker may omit sensitive details or financial information from this contract.	▪ Submit via the Entity-specific DE/EDE PME site at least thirty (30) days before commending the privacy and security audit during the planning phase. ▪ After CMS has received the SAP and auditor contract, CMS will schedule an audit kick-off call with the prospective web-broker and auditor. ▪ For any existing web-brokers, consistent with the ISCM Strategy Guide, this step is only required if the web-broker is changing auditors for its annual assessment.
Security and Privacy Assessment Report (SAR)	▪ The report should contain a summary of findings that includes ALL findings from the assessment to include documentation reviews, control testing, scanning, penetration testing, interview(s), etc. o Explain if and how findings are consolidated. o Ensure risk level determination is properly calculated, especially when weaknesses are identified as part of the Center for Internet Security (CIS) Top 18 and/or OWASP Top 10. ▪ The assessment must be conducted by an independent third-party auditor with experience outlined in the *Framework for Independent Assessment*. Among the experience required include familiarity with National Institute of Standards and Technology (NIST) standards, the Health Insurance Portability and Accountability Act (HIPAA), and other applicable federal privacy and cybersecurity regulations and guidance. ▪ Alternatively, the web-broker may reference existing audit results that address some or all of the assessment's requirements, assuming	▪ Submit via the Entity-specific DE/EDE PME site using the SAR template on CMS zONE[30] ▪ 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.

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

Document	Description	Submission Requirements
	the existing audit results were produced by a third-party auditor in conformity with the requirements described above. o If existing audit reports do not address all required elements of the assessment, the remaining elements must be addressed utilizing one of the first two assessment options. o If existing audit reports are utilized, the reports must have been based on assessment activities completed within the last year. ▪ The SAR should not include comments that describe the third-party assessor's process for verifying the requirement, unless there is a specific issue or concern with respect to the requirement that warrants raising the concern to CMS.	
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. [31]	▪ Submit via the Entity-specific DE/EDE PME site with the SAR.
Plan of Action and Milestones (POA&M)	▪ Submit a POA&M if its third-party auditor identifies any privacy and security compliance issues in the SAR. ▪ 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.	▪ POA&Ms with outstanding findings must be submitted monthly to CMS until all the findings from security controls assessments, security impact analyses, and continuous monitoring activities are resolved. Prospective Web-brokers can schedule their own time for monthly submissions of the POA&M, but must submit an update monthly to CMS until all significant or major findings are resolved. Thereafter, quarterly POA&M submissions are required as part of the ISCM activities. ▪ Submit via the web-broker's entity-specific DE/EDE PME site using the POA&M template on CMS zONE with the SAR.
Network and Component Vulnerability Scans	▪ A web-broker must submit the most recent three (3) months of its Vulnerability Scan Reports. ▪ All findings from vulnerability scans are expected to be consolidated in the monthly POA&M (the POA&M is expected to be updated monthly, if applicable, but only submitted as indicated in the following	▪ Submit via web-broker's entity-specific DE/EDE PME site with the SAR.

[31] Section V.b of the Web-broker Agreement contains additional information on the penetration testing requirements.

Document	Description	Submission Requirements
	row unless additional submissions are requested by CMS). ▪ Similar findings can be consolidated.	
Non-Exchange Entity System Security and Privacy Plan (NEE SSP) – if requested	▪ The NEE SSP must include complete and detailed Information about the prospective or existing Web-broker's implementation specifications of required security and privacy controls. ▪ The implementation of security and privacy controls must be completely documented in the SSP before the audit is initiated.	▪ Web-brokers are not required to submit the NEE SSP to CMS. However, CMS may request and review the NEE SSP. ▪ If requested to submit, web-brokers must use the NEE SSP template on CMS zONE.
Risk Acceptance Form	▪ The Risk Acceptance Form records the weaknesses that require an official risk acceptance from the organization's Authorizing Official. ▪ Before deciding to accept the risks, the relevant NEE's authorities should rigorously explore ways to mitigate the risks. ▪ Web-brokers must document accepted risks using the Risk Acceptance Form and submitted with the POA&M during the regular POA&M submission schedule.[32]	▪ Submit via the web-broker's entity-specific DE/EDE PME site using the Risk Acceptance Form on CMS zONE with the POA&M.

ii. Privacy and Security Auditor Standards

Web-brokers must contract with one or more qualified privacy and security auditors to conduct the privacy and security audit described in Section III.A, pursuant to 45 C.F.R. §§ 155.221(f), (g), and (h).[33] This section details the required and recommended experience, conflict of interest, and independence and objectivity standards for auditors.

A web-broker must enter into a written agreement with each independent auditor it contracts with to conduct the privacy and security audit per 45 C.F.R. § 155.221(g). Pursuant to its oversight authority under 45 C.F.R. § 155.220(c)(5) and Section X.k of the Web-broker Agreement, CMS may request a copy of all documentation related to a web-broker's engagement of its auditor(s) and the auditor(s)' work in relation to the engagement. Upon contracting with the auditor, the web-broker must submit a copy of the signed agreement or contract between the auditor(s) and the web-broker to CMS pursuant to Section IX.a of the Web-broker Agreement.

CMS will not provide web-brokers with specific recommendations of auditors to conduct a privacy and security audit. CMS encourages web-brokers to work with their trade associations or other interested groups to share and disseminate information about possible auditors that meet the criteria defined in these guidelines.

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

[33] Also see 45 CFR §§ 155.220(c)(6)(iv) and 155.221(b)(4)(ii).

iii. Privacy and Security Auditor Recommended Expertise

CMS strongly recommends that a web-broker select an auditor that has prior FISMA experience and/or is listed on the FedRAMP-certified third-party assessment organization website.[34] Prior FISMA experience is recommended in order for an auditor to appropriately assess a web-broker's compliance with the required privacy and security controls and produce a high-quality comprehensive Security and Privacy Controls Assessment Test Plan (SAP) and Security and Privacy Assessment Report (SAR).

iv. Auditor Conflict of Interest Standards

Pursuant to Section IX.b of the Web-broker Agreement, a web-broker that is contracting with an auditor to submit an audit to CMS must select an auditor who is free from any real or perceived conflicts of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence. A web-broker's auditor must disclose to HHS any financial relationship between the auditor and individuals who own or are employed by the web-broker or who own or are employed by the web-broker for which the auditor is conducting an audit, pursuant to 45 C.F.R. § 155.221(g)(4) and Section IX.b of the Web-broker Agreement.

v. Auditor Independence and Objectivity

A web-broker's auditor must remain independent and objective throughout the audit process . An auditor is independent if there is no perceived or actual conflict of interest involving the developmental, operational, and/or management chain associated with the web-broker's DE environment and the determination of security and privacy control effectiveness or business requirement compliance. The auditor's role is to provide an independent assessment of the compliance of the web-broker's DE environment and to maintain the integrity of the audit process. Upon submission of the audit, auditors will be required to attest to their independence and objectivity in completing the audit, and that neither the web-broker nor the auditor took any actions that might impair the objectivity of the findings in the audit. This disclosure must happen in the SAP for the auditor, and in the Web-broker Agreement for the web-broker. Otherwise, notice must be provided to CMS consistent with the notice provision of the Web-broker Agreement.

B. Web-broker Business Requirements

Web-brokers must comply with the business requirements identified in Exhibit 2 consistent with the Web-broker Agreement operational readiness requirements (at the time of publication, these requirements appear in Sections III and V of the Web-broker Agreement).[35] CMS will not execute a Web-broker Agreement with a web-broker until the web-broker has met all business requirements outlined in this subsection and the privacy and security requirements outlined in Section III.A of these guidelines. For additional information on the web-broker onboarding process, please review Section IV of these guidelines. For prospective web-brokers, the requirements in Exhibit 2 must be completed before CMS will approve a prospective web-broker to operate a DE environment in production. For existing web-brokers, a subset of the

[34] Available at: https://marketplace.fedramp.gov/#/assessors?sort=assessorName.

[35] Also see 45 CFR 155.220(c)(6) and 155.221(b)(4)(i).

requirements in Exhibit 2 will apply as part of the annual agreement renewal process as described in Section IV.B.

Exhibit 2: Required Business Documentation and Evidence for Web-broker Approval

Requirement	Description	Submission Requirements
Data Request Form	▪ The web-broker must provide license information, points of contact; third-party relationships; and other related data elements (including the National Producer Number (NPN) of the web-broker's designated representative that will complete Marketplace registration and training) to CMS. ▪ Consistent with Section III.a.5 of the Web-broker Agreement, web-brokers must provide an NPN of at least one designated representative, who is an AB that has completed registration and training with the Exchange. If an entity is an AB DE TP and does not have a designated representative during the onboarding process, the AB DE TP can provide this Designated Representative NPN separately prior to CMS activating the web-broker's Partner ID to operate in production.	▪ Submit via web-broker's entity-specific DE/EDE PME site.
CMS Data Services Hub (Hub) Testing	▪ The web-broker must complete end-to-end testing with the Hub to demonstrate a successful classic DE end-to-end enrollment.[36] ▪ For web-brokers that plan to offer only an EDE pathway, 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. However, if a web-broker intends to offer a classic DE pathway and an EDE pathway, the web-broker must also demonstrate successful completion of a classic DE end-to-end test case.	▪ Conduct testing consistent with web-broker testing instructions slide deck on CMS zONE for submission requirements (https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials) ▪ Notify directenrollment@cms.hhs.gov upon completing the end-to-end testing.
Web-broker Agreement	▪ The web-broker must complete all fields and sign the Web-broker Agreement for the applicable plan year.[37]	▪ Submit via web-broker's entity-specific DE/EDE PME site.

[36] For additional information about the Hub testing requirement, see web-broker testing instructions at the following link on CMS zONE: https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials. Prospective web-brokers are granted access to CMS zONE as part of the web-broker onboarding process, after participating in an informational interview.

[37] The Web-broker Agreement is effective from execution through the day before the first day of the next plan year's annual open enrollment period (OEP). See 45 C.F.R. § 155.410(e) for more information on the annual OEP.

Requirement	Description	Submission Requirements
	▪ The Web-broker Agreement for the current plan year is available at the following link on CMS zONE: https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials.	
Testing Environment	▪ The web-broker must maintain a testing environment that accurately represents the web-broker's DE production environment consistent with Section III.a of the Web-broker Agreement.	▪ N/A
Pre-Approval Website Review	▪ CMS will review a web-broker's website to ensure compliance with DE website display requirements and guidance. ▪ The web-broker must provide CMS with a set a of website test environment credentials that CMS can use to access the web-broker's website testing environment (i.e., pre-production environment) to complete the website review of the web-broker's DE environment. ▪ CMS may contact the prospective web-broker during testing if CMS encounters any blockers in the testing environment. ▪ CMS will prepare a technical assistance letter summarizing any compliance findings identified during the pre-approval website review, as well as designating which findings the web-broker must resolve prior to CMS approving the web-broker. CMS may conduct additional testing to confirm resolution of the findings. ▪ For prospective web-brokers, CMS's approval to use the DE pathway in production is contingent on the web-broker resolving findings identified by CMS during the pre-approval website review as requested by CMS.	▪ Upon request, submit website test environment credentials via web-broker's entity-specific DE/EDE PME site. ▪ Submit evidence of any resolved compliance findings consistent with CMS instructions, if applicable.

IV. Web-broker Onboarding and Renewal Processes

This section details the onboarding process for prospective web-brokers. Generally, CMS will not approve a web-broker to operate a DE environment in production until it satisfies all of the operational readiness requirements detailed in Section III of these guidelines.

CMS's approval of a prospective web-broker allows that web-broker to operate as a web-broker with a classic DE environment in production. If a prospective web-broker is concurrently seeking approval as an EDE Entity, the prospective web-broker must also satisfy the EDE program requirements to obtain CMS approval to operate an EDE environment in production.[38] A

[38] Section VI of these guidelines details operational readiness requirements where a web-broker may use EDE operational readiness requirements evidence to satisfy web-broker operational readiness requirements.

prospective web-broker can obtain CMS approval to operate a classic DE environment in production prior to obtaining CMS approval to operate an EDE environment in production.[39]

A. Prospective Web-broker Onboarding Process

CMS will approve a prospective web-broker once a prospective web-broker has met the operational readiness requirements to CMS's satisfaction. As noted above, if a web-broker is concurrently seeking approval as an EDE Entity, the prospective web-broker must also satisfy the EDE program requirements to obtain CMS approval to operate an EDE environment in production.

CMS accepts web-broker onboarding requests on a rolling basis. The process to obtain CMS approval as a web-broker may take several months from the point the web-broker has submitted its operational readiness review documentation.[40] This does not include the time that it would take a prospective web-broker to develop its DE environment and prepare the required operational readiness review documentation, including the privacy and security audit. Prospective web-brokers should consider this approval time when evaluating anticipated go-live timeframes. CMS does not guarantee any review or approval timelines. CMS cannot estimate go-live timeframes for a prospective web-broker.

Exhibit 3 describes the typical web-broker onboarding process.

Exhibit 3: Web-broker Onboarding Process

Steps	Description	Submission Requirements
Submit Initial Notice of Intent	▪ The prospective web-broker notifies CMS that it is interested in pursuing onboarding as a web-broker for classic DE and/or EDE. ▪ CMS provides general information about DE and EDE via email. ▪ Prospective web-broker confirms intent to continue with onboarding.	▪ Email directenrollment@cms.hhs.gov with a notice of intent to become a web-broker.
Participate in Informational Interview with CMS	▪ CMS will schedule an informational interview with CMS and the prospective web-broker. During this interview, CMS will ask the web-broker questions about its operations, plans to operate as a classic DE or EDE web-broker, and other operational or oversight-related questions. ▪ CMS will provide information about DE and the onboarding process, as well as the approval requirements and expectations consistent with those defined in this document. ▪ After the call, CMS will send a variety of resources, including the instructions to request access to the	▪ CMS will request times when the prospective web-broker is available to meet and initial operational information prior to the informational interview.

[39] However, in this situation, if a web-broker is using documents from its EDE assessment to meet web-broker operational readiness requirements (as detailed in Section VI of these guidelines), CMS will evaluate whether the web-broker has sufficiently demonstrated those requirements from its EDE assessment prior to approving the web-broker to operate its classic DE environment in production prior to approval to operate its EDE environment in production.

[40] The expected timelines for obtaining approval as an EDE Entity are discussed in more detail in the EDE Guidelines (see, *supra*, note 7).

Steps	Description	Submission Requirements
	CMS zONE Web-broker Community and the Web-broker Agreement for the applicable plan year.	
Integrate with the CMS Data Services Hub (DSH) and DE APIs	▪ The prospective web-broker submits a Hub Onboarding Form to the DSH team to establish a connection to the DE APIs in the FFE testing environment. ▪ Using API companion guides available on CMS zONE, the prospective web-broker will then commence developing its DE environment and integrating with the applicable APIs.	▪ Submit the Hub Onboarding Form to the DSH team to begin the connection to the Hub, as well as any required materials (e.g., SSL certificates).
Submit Business Requirements Evidence	▪ Consistent with Exhibit 2, the prospective web-broker must submit the following required documentation: a data request form, a signed Web-broker Agreement, and demonstrate a successful classic DE end-to-end test enrollment. ▪ Web-brokers must submit this documentation at any time prior to submitting the privacy and security audit.	▪ Submit via the prospective web-broker's entity-specific DE/EDE PME site.
Submit Privacy and Security Requirements Evidence	▪ The prospective web-broker must submit a privacy and security assessment consistent with Section III.A. ▪ Exhibit 1 details the specific submission requirements and deadlines for each element of the privacy and security audit package. ▪ Prior to conducting the privacy and security audit, consistent with Exhibit 1, the prospective web-broker must submit an SAP and auditor contract. After doing so, CMS will schedule an audit kick-off call to confirm the scope of the audit and answer any questions from the prospective web-broker or auditor.	▪ Submit via the prospective web-broker's entity-specific DE/EDE PME site. ▪ CMS strongly recommends prospective web-brokers submit the privacy and security audit by the last business day in June of the applicable year to mitigate the risk of any delays to the approval process prior to the Open Enrollment Period (OEP).
Pre-Approval Website Review	▪ Consistent with Exhibit 2, a DE Entity must provide website test environment credentials in response to a request from CMS. CMS will request testing credentials only after the prospective web-broker has submitted the privacy and security audit.	▪ Submit website test environment credentials via prospective web-broker's entity-specific DE/EDE PME site, as requested by CMS.
Approval	▪ While reviewing the prospective web-broker's submitted evidence for the privacy and security requirements (Exhibit 1) and business requirements (Exhibit 2), CMS will identify any issues that the prospective web-broker must resolve prior to approval. ▪ Once the web-broker has resolved any CMS-identified issues to CMS' satisfaction, CMS will countersign the prospective web-broker's submitted Web-broker Agreement and approve the web-broker to operate a classic DE environment in production. If the prospective web-broker has simultaneously met the requirements to operate as an EDE Entity, CMS will approve the web-broker to operate an EDE environment in production.	▪ Submit required resolution evidence via the prospective web-broker's entity-specific DE/EDE PME site, as requested by CMS.

Steps	Description	Submission Requirements
	▪ Upon approval, CMS will add the web-broker's name to the Web-broker Public List. The Public List contains the names of all active web-brokers operating with the FFE.[41] Note: It may take a week or more for CMS to post the update to its public-facing webpage.	

B. Prospective Web-broker Approval Considerations

Prospective web-brokers must submit the required documentation detailed in Section III and complete the onboarding process detailed in Exhibit 3 before CMS will consider approving the prospective web-broker to operate its DE environment in production.

CMS reviews all materials submitted by prospective web-brokers and may contact prospective web-brokers with any questions or requests for further documentation. CMS does not guarantee any web-broker onboarding or approval timeframes.

For a prospective web-broker that intends to use only the classic DE pathway, CMS strongly recommends that the web-broker submit the privacy and security documentation by the last business day in June for the applicable year. This will mitigate the risk of any delay in completing the onboarding process prior to the start of the Open Enrollment Period (OEP) for that year. Prospective web-brokers that submit the required documentation after the last business day in June may not receive CMS approval in time to operate during the OEP.

For a prospective web-broker that intends to participate in EDE, the web-broker may submit the privacy and security documentation consistent with the requirements in Section VI.

For a web-broker that intends to use classic DE, upon demonstrating compliance with the web-broker operational readiness requirements for approval as a web-broker consistent with these guidelines, CMS will enable a web-broker's access in production to use the DE web services. If a web-broker is only seeking to use the EDE pathway, CMS will enable the web-broker's access in production to use the FFE web services after the prospective web-broker has met both the web-broker operational readiness requirements and the EDE operational readiness requirements for the web-broker's intended EDE arrangement type.[42]

V. Existing Web-broker Agreement Renewal Processes

Each year, web-brokers that have been approved will need to proceed through the Web-broker Agreement renewal process. CMS will only renew an existing web-broker's Web-broker Agreement for the subsequent plan year if the web-broker has submitted an annual ISCM audit (Section III.A) and the subset of business requirements listed in Exhibit 4. Each year, prior to the expiration of the active Web-broker Agreement for the current plan year, CMS will provide

[41] The current Public List is available on the Direct Enrollment and Enhanced Direct Enrollment Resources webpage: https://www.cms.gov/programs-and-initiatives/health-insurance-marketplaces/direct-enrollment-and-enhanced-direct-enrollment.

[42] Refer to Section VI for more information on a prospective web-broker's concurrent approval to operate as a web-broker and EDE Entity.

notice via email of the specific processes and documentation needed to complete Web-broker Agreement renewal for the upcoming plan year.

Exhibit 4: Business Requirements for Annual Agreement Renewal

Requirement	Description	Submission Requirements
Data Request Form	▪ Provide license information, points of contact; third-party relationships; and other related data elements (including the National Producer Number (NPN) of the web-broker's designated representative that has completed Marketplace registration and training for the appropriate plan year for which the agreement is being renewed) to CMS.	▪ Submit via web-broker's entity-specific DE/EDE PME site.
CMS Data Services Hub (Hub) Testing	▪ Complete end-to-end testing with the Hub[43] . ▪ For web-brokers that plan to offer only an EDE pathway, 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. However, if a web-broker intends to offer a classic DE pathway and an EDE pathway, the web-broker must also demonstrate successful completion of a classic DE end-to-end test case. ▪ Note: CMS requires end-to-end testing for agreement renewal only if the web-broker does not have a history of completing an enrollment in the prior plan year via DE.	▪ See web-broker testing instructions slide deck on CMS zONE for submission requirements (https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials).
Web-broker Agreement	▪ Complete all blank fields and sign the Web-broker Agreement for the applicable plan year[44].	▪ Submit via web-broker's entity-specific DE/EDE PME site.

Web-brokers who fail to complete the Web-broker Agreement renewal process by the expiration date of the current Web-broker Agreement will have their production access to the DE web services terminated. In order to receive CMS approval as a web-broker again, the web-broker must go through the onboarding process again and satisfy the web-broker privacy and security (Exhibit 1) and business audit (Exhibit 2) requirements detailed in these guidelines.

[43] For additional information about the Hub testing requirement, see web-broker testing instructions at the following link on CMS zONE: https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials. CMS grants prospective web-brokers access to CMS zONE as part of the web-broker onboarding process.

[44] The Web-broker Agreement is effective from execution through the day before the first day of the next plan year's annual open enrollment period (OEP). *See* 45 C.F.R. § 155.410(e) for more information on the annual OEP.

VI. Web-broker Operational Readiness Requirements and Related EDE Requirements

This section details scenarios and the accompanying requirements where a web-broker—either existing or prospective—may be able to satisfy web-broker operational readiness review requirements with documentation submitted to satisfy the EDE operational readiness review requirements detailed in the EDE Guidelines.

A. Web-broker Approval Concurrent with EDE Approval

If a prospective web-broker has submitted an EDE audit package as a prospective EDE Entity, CMS can approve the prospective web-broker as both a web-broker and EDE Entity at the same time. This process will require the prospective web-broker complete the requirements for both programs to CMS's satisfaction, including submitting one or more privacy and security audits, depending on the web-broker's implementation of EDE and classic DE (if applicable), as described in more detail in Section VI.B.[45] In general, CMS must approve a prospective web-broker as a web-broker prior to (or concurrent with) approval to operate as an EDE Entity. There are exceptions to this rule if a prospective web-broker is operating as a non-web-broker EDE Entity (e.g., a QHP issuer DE Technology Provider).[46]

B. Satisfaction of the Web-broker Privacy and Security Audit Operational Readiness Requirements Based on an EDE Privacy and Security Audit Submission

If an existing or prospective EDE Entity intends to become a CMS-approved web-broker, the EDE Entity may be able to satisfy some of the web-broker privacy and security audit operational readiness review requirements[47] detailed in these guidelines through meeting the requirements to obtain or maintain CMS approval as an EDE Entity.[48]

Specifically, CMS will allow an existing or prospective EDE Entity to use all or part of its EDE privacy and security audit to satisfy the web-broker privacy and security audit operational readiness review requirement under certain conditions. In general, the audit must have 1) been completed within the past year, 2) assessed all applicable classic DE and EDE environments and functionality, and 3) assessed the full scope of web-broker privacy and security requirements and controls.

For web-brokers that meet those criteria, CMS will accept an attestation from the web-broker as outlined in Section VI.B.iv of these guidelines. Web-brokers must submit the attestation via their entity-specific DE/EDE PME site with the EDE privacy and security audit documentation.

---

[45] See *supra* note 15.

[46] As described in Section II.E, in this scenario, a QHP issuer DE technology provider operating as an EDE Entity would be prohibited from arrangements and functionality described in Section II.E, until CMS approved the QHP issuer DE technology provider to also operate as a web-broker.

[47] For the operational readiness review business requirements, there is a limited opportunity for a prospective web-broker to satisfy the web-broker operational readiness review requirements with documentation submitted for an EDE operational readiness review business audit. As noted in Exhibit 2, web-brokers that intend to operate as an EDE Entity and do not intend to use the classic DE pathway can satisfy the web-broker end-to-end testing requirement by completing an enrollment via the EDE pathway, as demonstrated during testing required to receive approval to use the EDE pathway.

[48] See *supra* note 7.

i. Privacy and Security Audits for Prospective and Existing Primary EDE Entities for Web-broker Approval

This section details several possibilities for a prospective or existing primary EDE Entity to use an EDE privacy and security audit for satisfying the web-broker privacy and security audit operational readiness review requirement.

An existing or prospective primary EDE Entity that seeks approval to use both EDE and classic DE as a web-broker may use its initial EDE privacy and security audit[49] or its most recent ISCM Strategy Guide submission, whichever is most recent, to meet the web-broker privacy and security audit operational readiness review requirement only if both the classic DE Environment and EDE Environment are within the same audit boundary for the EDE ISCM/privacy and security audit. A web-broker that intends to use its EDE privacy and security audit to satisfy the web-broker privacy and security audit operational readiness review requirement must submit an attestation to document and explicitly state this intention, consistent with Section VI.B.iv.

Alternatively, an existing or prospective primary EDE Entity that intends to only use an EDE environment as a web-broker—and that does not maintain a classic DE environment—may use its EDE privacy and security audit or its most recent ISCM Strategy Guide submission, whichever is most recent, to satisfy the web-broker privacy and security audit operational readiness review requirement. A web-broker that intends to only use an EDE environment and does not maintain a classic DE environment must submit an attestation to document and explicitly state this intention, consistent with Section VI.B.iv.

If the EDE and classic DE environments and functionality are not within the same audit boundary, the web-broker must submit a privacy and security audit for each environment that assesses the relevant privacy and security controls (e.g., the primary EDE Entity privacy and security controls for the EDE environment and the web-broker privacy and security controls for the classic DE environment).

ii. Privacy and Security Audits for Prospective and Existing Hybrid Non-Issuer Upstream EDE Entities for Web-broker Approval

This section details several possibilities for a prospective or existing hybrid, non-issuer upstream EDE Entity to use an EDE privacy and security audit for satisfying the web-broker privacy and security audit operational readiness review requirement.

An existing or prospective hybrid non-issuer EDE Entity that intends to maintain both classic DE and EDE Environments as a web-broker may be able to use its initial EDE privacy and security audit or its most recent EDE ISCM Strategy Guide submission, whichever is most recent, to meet a portion or all of the web-broker privacy and security audit operational readiness review requirement under the following conditions.

If the existing or prospective hybrid non-issuer upstream EDE Entity's classic DE and EDE environments and functionality will exist within the same audit boundary, the web-broker may

[49] If a prospective primary EDE Entity intends to use its initial EDE privacy and security audit to satisfy the web-broker privacy and security audit operational readiness review requirements or the web-broker ISCM Strategy Guide privacy and security audit, the initial EDE privacy and security audit must be deemed complete by CMS. Please review the EDE Guidelines for the applicable year description of the Audit Completeness Review standards. See *supra* note 15. The initial EDE privacy and security audit must also have been completed within the last year.

submit one audit that evaluates 1) all applicable controls for the web-broker privacy and security audit operational readiness review requirements and 2) all applicable controls for the hybrid non-issuer upstream EDE Entity privacy and security audit operational readiness review requirements. The web-broker privacy and security controls must include any applicable controls that the auditor did not evaluate for the hybrid non-issuer upstream EDE Entity privacy and audit (e.g., any controls the web-broker, in its upstream arrangement, inherited from the primary EDE Entity and therefore the auditor did not fully evaluate the controls). A web-broker that intends to use one audit to satisfy both the web-broker privacy and security audit operational readiness review requirement and the hybrid non-issuer upstream EDE Entity privacy and security audit operational readiness review requirements must submit an attestation to document and explicitly state this intention, consistent with Section VI.B.iv.

If a prospective web-broker will operate only as a hybrid non-issuer upstream EDE Entity using an EDE environment and functionality provided by a primary EDE Entity, and the prospective web-broker does not intend to maintain a classic DE environment, then the web-broker may use its EDE hybrid non-issuer upstream EDE Entity privacy and security audit to satisfy the web-broker privacy and security audit operational readiness review requirement. The primary EDE Entity may also provide a classic DE environment in this arrangement; but the web-broker may not maintain its own, independent classic DE environment without meeting the web-broker privacy and security audit operational readiness review requirements. A web-broker that intends to only use an EDE environment and will not maintain a classic DE environment must submit an attestation to document and explicitly state this intention, consistent with Section VI.B.iv.

If the classic DE and EDE environments are not within the same audit boundary, the web-broker must submit a privacy and security audit for each environment that assesses the appropriate privacy and security controls (e.g., a web-broker privacy and security audit that evaluates the classic DE environment and functionality and a hybrid non-issuer upstream EDE Entity privacy and security operational readiness review audit that evaluates the EDE environment and functionality).

iii. Prospective Primary EDE Entity Privacy and Security Audit Requirements and the EDE Audit Submission Window

This section describes an option available in the specific circumstance where a prospective primary EDE Entity—that is also a prospective web-broker—has its EDE privacy and security audit submission rejected as incomplete during the audit submission window. If the entity intends to use its EDE privacy and security audit submission that CMS deemed incomplete to satisfy the web-broker privacy and security audit operational readiness review requirement, as described in Section VI.B.i, the entity may resubmit the incomplete audit during the audit submission window consistent with the EDE Guidelines requirements, if the audit submission window is still open.

If the prospective primary EDE Entity is unable to submit an updated complete EDE privacy and security audit within the audit submission window, and the entity still intends to pursue approval as a classic DE web-broker, the entity may resolve the completeness issues identified by CMS and resubmit the privacy and security audit to satisfy the requirement for web-broker approval only. The entity does not need to switch to the SSP template prior to resubmitting this documentation; it may resubmit the documentation using the same EDE templates for the initial EDE submission. In this scenario, the entity may be approved to operate, or continue operating,

as a web-broker, but the entity 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.

iv. Web-broker Attestation for Using an EDE Privacy and Security Audit to Satisfy Web-broker Privacy and Security Audit Operational Readiness Review Requirements

Any web-broker that intends to pursue the flexibilities offered in these guidelines and use an EDE privacy and security audit to satisfy the web-broker privacy and security audit operational readiness review requirements must submit an attestation to CMS detailing the web-broker's intent and justification. This includes, but is not limited to, situations where a web-broker intends to only use an EDE environment and will not maintain a classic DE environment, as well as situations where the web-broker intends to use both a classic DE and EDE environment. The attestation must state which of the previous scenarios outlined in Section VI.B of these guidelines applies to the web-broker's situation. The attestation must be submitted on company letterhead and must be signed and dated by an authorized company representative.

Web-brokers must submit the attestation via their entity-specific DE/EDE PME site at the time of its EDE security and privacy audit submission. Existing web-brokers that assert their EDE assessments included 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., the SSP).

VII. Approved Web-broker Monitoring and Oversight

CMS regularly conducts oversight and monitoring of web-broker classic DE and EDE environments pursuant to 45 C.F.R. § 155.220(c)(5). This may include reviews of test environments or production websites maintained by web-brokers for compliance with applicable program requirements. CMS may suspend a web-broker's production access to the Hub if a web-broker fails to provide website test environment credentials in response to a request from CMS, consistent with Sections V.a and X.l of the Web-broker Agreement.

Generally, web-brokers are required to comply with the applicable requirements in 45 C.F.R. §§ 155.205(c), 155.220, 155.260, and 155.221. CMS strongly recommends prospective web-brokers review the regulatory requirements prior to beginning the onboarding process. Additionally, web-brokers must comply with the program requirements in the Web-broker Agreement and the operational technical specifications outlined in applicable program guidance.[50] Web-brokers that operate as EDE Entities must also comply with the program requirements in the EDE Business Agreement and the operational technical specifications in applicable program guidance, including the EDE Guidelines.

[50] CMS posts web-broker program guidance at the following link: https://www.cms.gov/programs-and-initiatives/health-insurance-marketplaces/direct-enrollment-and-enhanced-direct-enrollment. Web-brokers should also review the annual Federally-facilitated Exchange (FFE) Enrollment Manual. The latest version of the FFE Enrollment Manual available at the time of publication is available at the following link: https://www.cms.gov/files/document/ffe-enrollment-manual-2023-5cr-071323.pdf.

VIII. DE/EDE Entity Program Management Environment (PME) Site for Document Submission

CMS requires each prospective and existing web-broker to submit documents to CMS via its DE/EDE Entity PME Site. After the Entity informs CMS that it has entered into an agreement with its auditor(s), CMS will provide the Entity with instructions to establish a DE/EDE Entity PME Site that the Entity will use to access and upload documents to the PME site. CMS will also provide written instructions for using the DE/EDE Entity PME Site via email at that time. CMS will not require DE Entities to encrypt documents containing proprietary information before uploading them to the PME site.

IX. Resources

A. Help Desk

In addition to hosting weekly webinars, which include time for interactive questions and answers, CMS currently manages multiple web-broker-facing help desks to address questions; help web-brokers and prospective web-brokers 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 [Entity name] on [Topic]." Emails to the FEPS Help Desk will be routed to the appropriate team.
- 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 Hubsupport@sparksoftcorp.com and CMS_FEPS@cms.hhs.gov with the subject line "DE: API Q for [Entity name] on [Topic]." Emails to the Hub Help Desk will be routed to the appropriate team.
- A DE Entity with a policy or compliance question related to the privacy and security assessment, business requirements, the onboarding process, web-broker program guidance, or the Web-broker Agreement should e-mail DE Support at directenrollment@cms.hhs.gov with the subject line "Web-broker Q for [Entity name] on [Topic]." CMS may not respond to policy questions on either of these topics if they are not sent to DE Support.

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

- Your contact information (e-mail and phone number).
- Name of your organization and your organization's CMS-issued Partner ID (if the web-broker has an existing 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).) for troubleshooting when applicable. If the XMLs/JSONs include PII, 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.

B. Webinars

CMS presents important DE updates through the Issuer Technical Workgroup (ITWG) webinar on Tuesdays from 3:00 PM to 4:30 PM ET. The ITWG call is open to all web-brokers and issuers operating in the FFEs or SBE-FPs. 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 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.[51]

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 these guidelines, 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.

Web-broker privacy and security templates, as well as the Penetration Testing Notification Form, NEE Risk Acceptance Form, and NEE Decommissioning Plan and Close Out Letter, are the same as EDE privacy and security templates, available on CMS zONE at the following link: https://zone.cms.gov/document/privacy-and-security-audit.

CMS has this webpage is accessible by members of the Private Issuer Community (for issuers) the Web-Broker Community (for web-brokers), and the EDE Auditor Community (for auditors working with DE Entities) 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.

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.

[51] In order to gain access to the registration link for the Issuer Technical Workgroup webinar, web-brokers, after gaining access to CMS zONE, should join the Enrollment Community. CMS posts information about the enrollment community at the following link: https://zone.cms.gov/document/enrollment-community. Note: If you have already registered for this webinar series, please use the login information sent to you by zoom.gov.

Unless otherwise specified, any guidance or requirements stated as forthcoming in these guidelines are expected to be made available through the CMS zONE Communities for DE.

D. REGTAP

CMS will make various web-broker-, EDE-, and agent/broker-related trainings and a list of essential resources available via REGTAP.[52]

E. Additional Guidance

- Federally-facilitated Exchange (FFE) Enrollment Manual: https://www.cms.gov/files/document/ffe-enrollment-manual-2023-5cr-071323.pdf.[53]
- 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/. EDE 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 SHOP coverage operations. CMS will provide information to EDE Entities if changes are made in the future.
- Privacy Act of 1974: http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/PrivacyActof1974.html.
- The Current Acceptable Risk Safeguards (ARS) documentation: https://www.cms.gov/research-statistics-data-and-systems/cms-information-technology/informationsecurity/information/acceptable-risk-safeguards-50x.
- MCCIIO Regulations and Standards: https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/index.html.
- HHS Guidance Submissions: https://www.hhs.gov/guidance/.
- CMS Risk Management Handbook (RMH) Chapter 08: Incident Response: https://www.cms.gov/files/document/rmh-chapter-08-incident-response.pdf.

[52] REGTAP can be accessed at the following link: https://www.regtap.info/.
[53] Note: CMS updates the FFE Enrollment Manual annually.