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:** December 10, 2019
**From:** Center for Consumer Information and Insurance Oversight (CCIIO)
**Title:** Health Insurance Exchange Guidance
**Subject:** Updated Direct Enrollment Web-broker Program Participation Requirements

## I. Background

The Centers for Medicare & Medicaid Services (CMS) is establishing new requirements for prospective web-brokers onboarding on or after January 1, 2020 (prospective web-brokers). This is also for 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). This guidance is applicable to prospective and existing 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 also applies to both prospective and existing web-brokers using the classic Direct Enrollment (DE) pathway and those using the Enhanced Direct Enrollment (EDE) pathway.[1]

Pursuant to 45 C.F.R. § 155.221(b)(4), DE Entities, 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.[2] 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).[3] Further details are provided in Exhibit 1.

[1] See Section V. Considerations for Web-brokers That Are Prospective or Existing EDE Entities, for specific information on how the requirements may impact web-brokers approved for or seeking to be approved for EDE.

[2] DE Entities are web-brokers and QHP issuers using DE 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.

[3] Also see 45 C.F.R. §§ 155.220(d)(3) and 155.260(b).

**Exhibit 1. Current Privacy and Security Requirements for Web-brokers**

| Requirement | Description |
|---|---|
| Privacy and Security Control Implementation | ▪ Web-brokers must implement the 159 critical security and privacy controls[4] specified in the Web-broker Agreement consistent with the NEE SSP.<br>– The NEE SSP contains comprehensive security and privacy control objectives for all aspects of the DE program (i.e., classic DE and EDE). The Web-broker Agreement requires implementation of 159 critical controls that map to the control objectives in the NEE SSP.<br>▪ It is strongly recommended that web-brokers implement all controls in the NEE SSP.<br>▪ Web-brokers are required to assess the 159 critical controls in the Web-broker Agreement, per Appendix A subsection: Annual Security and Privacy Attestation (SPA) of the Web-broker Agreement.<br>– 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. |

As discussed in more detail in the following sections, starting January 1, 2020, prospective and existing web-brokers will be 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 will be required to respond to an annual data request and may be required to complete additional testing. Prospective web-brokers will also be required to undergo a pre-approval website review that will occur before their respective websites can go live and be made available to consumers.

## II. Updated Operational Readiness Review Requirements

Starting January 1, 2020, prospective and existing web-brokers must comply with the following business requirements:

- **Annual data request** for updated licensure information, points of contact, third-party relationships, and other related data elements.
- **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.

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.

The Web-broker Agreement is effective from execution through the day before the first day of the following annual open enrollment period (OEP) and must be re-signed annually. Prospective and existing 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 web services 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

[4] As detailed in Section V., additional privacy and security controls apply to web-brokers participating in EDE.

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 must also comply with the following updated onboarding requirements:

- **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 the DE Help Desk, 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 application program interfaces (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.
- **Timing of Execution of the Web-broker Agreement:** Prospective web-brokers will build their DE websites and complete technical onboarding (including the pre-approval website review) prior to receiving a countersigned Web-broker Agreement from CMS. After an initial interview, prospective web-brokers will submit the signed 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.[5]

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*, available at: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/Processes-Becoming-Web-broker.pdf. CMS will conduct ongoing oversight of web-brokers, including regular reviews of web-broker websites for compliance with website display guidance. Web-brokers should maintain a testing environment that accurately represents their DE production environment.

## III. New Operational Readiness Review Required Privacy and Security Documentation

Starting January 1, 2020, web-brokers will no longer 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, prospective and existing web-brokers will be required to submit the information outlined in Exhibit 2 to CMS.[6] See Section IV. Deadlines and Final Approval for details on the timing and deadline for submission of this documentation.

[5] 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.

[6] These documents may also be requested from web-brokers who currently participate in classic DE or EDE 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).

**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[7] |
| 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.<br>– Explain if and how findings are consolidated.<br>– 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.<br>▪ 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.<br>▪ Assessment options: The report may be prepared by:<br>– A third-party auditor (recommended); or<br>– Internal staff, provided that:<br>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.<br>o They are not involved in the developmental, operational, and/or management chain associated with the system that is the subject of the assessment.<br>▪ 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.<br>– 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. | ▪ Submit via the secure portal using the SAR template on CMS zONE[8] |
| Network and Component Vulnerability Scans | ▪ A web-broker must submit the most recent three (3) months of its Vulnerability Scan Reports.<br>▪ All findings from vulnerability scans are expected to be consolidated in the monthly POA&M.<br>▪ Similar findings can be consolidated. | ▪ Submit via the secure portal |

[7] Web-brokers that do not already have a secure portal account must e-mail 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.

[8] 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 |
|---|---|---|
| Plan of Action and Milestones (POA&M) | ▪ Submit a POA&M if its assessor identifies any privacy and security compliance issues in the SAR.<br>▪ Ensure all open findings from the SAR have been incorporated into the POA&M.<br>▪ Explain if and how findings from the SAR were consolidated on the POA&M; include SAR reference numbers, if applicable.<br>▪ Ensure the weakness source references each source in detail to include type of audit/assessment and applicable date range.<br>▪ Ensure the weakness description is as detailed as possible to include location/server/etc., if applicable.<br>▪ Ensure scheduled completion dates, milestones with dates, and appropriate risk levels are included. | ▪ Submit via the secure portal using the POA&M template on CMS zONE |
| 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.<br>▪ If requested to submit, web-brokers must use the NEE SSP template on CMS zONE. |

Prospective and existing web-brokers must submit the complete set of documents outlined in Exhibit 2 to CMS. 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.

## IV. Deadlines and Final Approval

Prospective and existing web-brokers must submit the privacy and security documentation discussed in Section III, New Operational Readiness Review Required Privacy and Security Documentation 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 2021 OEP.

Prospective and existing web-brokers must meet the updated operational readiness review requirements in Section II, Updated Operational Readiness Review Requirements as part of the web-broker onboarding or renewal processes, as applicable.

CMS will review all submitted materials and reach out to web-brokers with any questions or requests for further documentation. CMS does not guarantee onboarding or renewal timeframes. CMS will notify prospective and existing web-brokers once their privacy and security documents are deemed complete and once these entities have met all other requirements in this guidance.

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

Web-brokers that are currently approved to use EDE or that intend to seek approval to participate in EDE should consider how the privacy and security requirements outlined in this guidance may be relevant in the context of the assessments they have completed or intend to complete with respect to EDE.

The NEE SSP, SAR, and POA&M templates referenced in this guidance are largely the same as the templates used for EDE. However, web-brokers seeking to participate in EDE must implement all the security and privacy controls documented in the NEE SSP. CMS strongly recommends all web-brokers implement all of the controls in the NEE SSP; however, web-brokers only participating in classic DE are only required to implement and assess the 159 critical controls documented in the Web-broker Agreement.

Web-brokers approved 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 included all classic DE environments and functionality. 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., an SSP). Web-brokers approved to participate in EDE should contact the DE Help Desk (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 specifically 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.

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 the DE Help Desk at directenrollment@cms.hhs.gov with the subject line “Web-broker Q for [Partner] on [Topic].”

### *B. Webinars*

CMS presents important DE and EDE 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/EDE community on developments related to DE and offer interactive question and answer time at the end of each session.

The call-in information for the weekly ITWG webinar is as follows:

- One-time Webinar Registration URL for series through February 2020: (If you have already registered for this webinar series please use the login information sent to you by webex.com) https://cl.s7.exct.net/?qs=a7d10599807267b9d58942a62db2a4d0f0027993bdcdbdab6849b47275536b9ec10dcf862d2d9ce4930524c7fcec569b

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, guidelines, such as those referenced in this document, 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.

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

### *D. REGTAP*

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

## E. *Additional Guidance*

- *Federally-facilitated Exchange (FFE) 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-PY19PY20.pdf*
- *Frequently Asked Questions (FAQs) Regarding the 2020 Audit Submission Timeline for Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment (EDE) Pathway*: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/FAQ-EDE-CY2020.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.