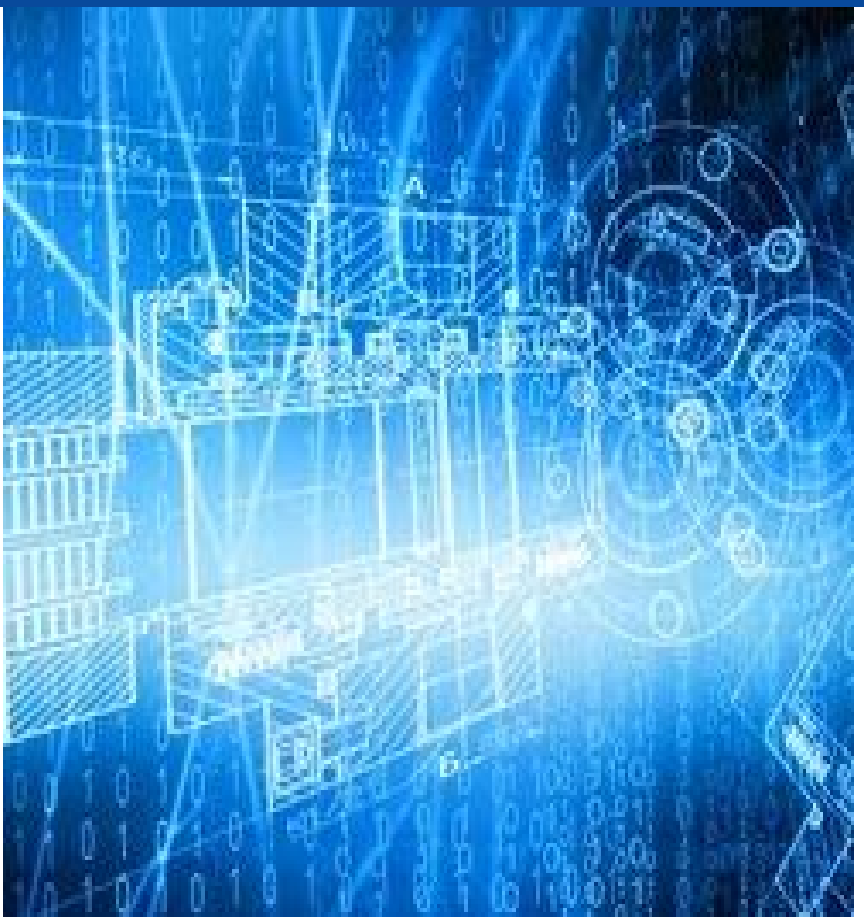
CENTERS FOR MEDICARE & MEDICAID SERVICES
CENTER FOR CONSUMER INFORMATION & INSURANCE OVERSIGHT

Updated Direct Enrollment (DE) Web-broker Program Participation Requirements



An Overview for Prospective and Existing Web-brokers

December 10, 2019

This communication was printed, published, or produced and disseminated at U.S. taxpayer expense.

The information provided in this presentation is not intended to take the place of the statutes, regulations, and formal policy guidance that it is based upon. This presentation summarizes current policy and operations as of the date it was shared. Links to certain source documents may have been provided for your reference. We encourage persons attending the presentation to refer to the applicable statutes, regulations, and other guidance for complete and current information.

Intended Audience and Purpose

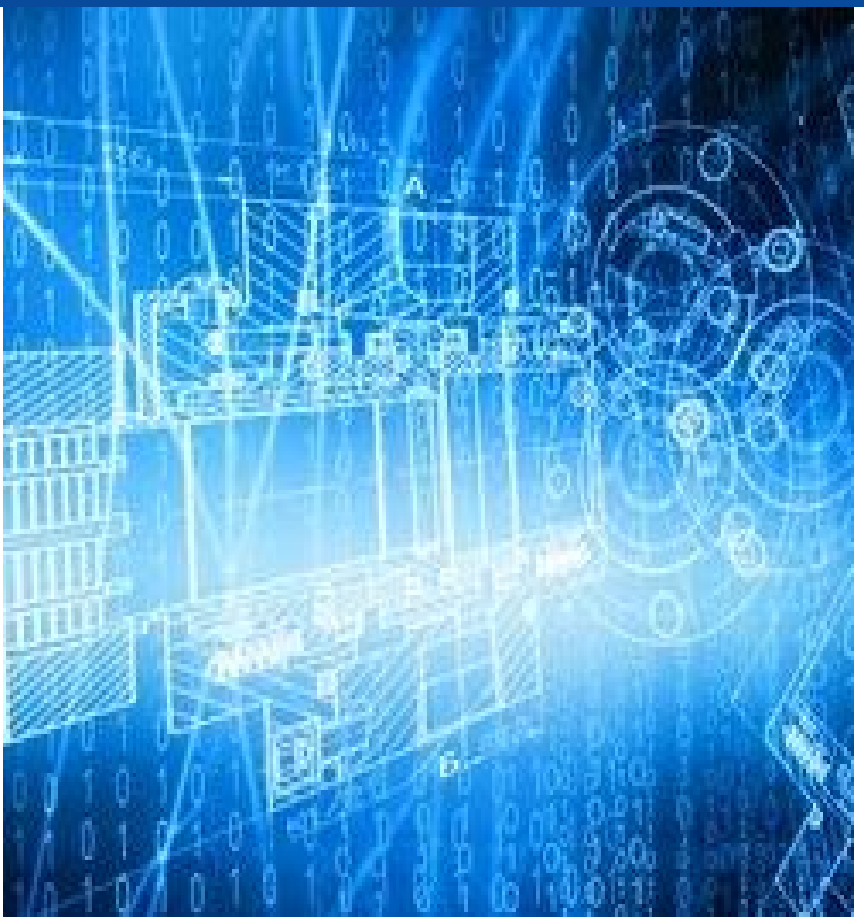
- The intended audiences for this presentation are as follows:
  - **Prospective web-brokers** onboarding on or after January 1, 2020
  - **Existing web-brokers** that will complete their Web-broker Agreement renewal in 2020 in order to continue to operate as web-brokers for plan year (PY) 2021
- This webinar is applicable to web-brokers using the classic Direct Enrollment (DE) and Enhanced Direct Enrollment (EDE) pathways that operate in states using the federal platform, which include Federally-facilitated Exchanges (FFEs) and State-based Exchanges on the Federal Platform (SBE-FPs) (collectively referred to as Marketplaces).
- The purpose of this presentation is to provide an overview of the new guidance outlining updated operational readiness review requirements for web-brokers.
  - The information in this presentation is based on the guidance on *Updated Direct Enrollment Web-broker Program Participation Requirements* published by CMS on December 10, 2019, available at: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/Guidance-on-Updated-DE-Web-broker-Program-Requirements.pdf
  - **Web-brokers should carefully review this guidance.**

Agenda

- Introduction
- New Operational Readiness Review Requirements (Business)
- New Operational Readiness Review Required Privacy and Security Documentation
- Deadlines and Final Approval
- Information for EDE Entities
- Resources
- Q&A

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF TECHNOLOGY SOLUTIONS

Introduction



Background

- 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.

Background: Web-broker Onboarding and Agreement Renewal

- Web-brokers may onboard year-round.
- 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 email renewal instructions and other materials to existing web-brokers prior to the annual OEP. CMS will email instructions and other materials to prospective web- brokers as part of the onboarding process.

Background: Current Privacy and Security Requirements for Web-brokers

- Web-brokers must 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 Web-broker Agreement and the *Non-Exchange Entity System Security and Privacy Plan* (NEE SSP) as described below.
- All documents referenced are available on CMS zONE: https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials (access limited to current issuers and web-brokers)

Requirement	Description

Privacy and Security Control Implementation	• Web-brokers must implement the 159 critical security and privacy controls* specified in the Web-broker Agreement consistent with the NEE SSP.
	  ◦ 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.
	• It is strongly recommended that web-brokers implement all controls in the NEE SSP.
	• 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.
	  ◦ 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.

** Additional privacy and security controls apply to web-brokers participating in EDE.*

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF TECHNOLOGY SOLUTIONS

New Operational Readiness Review Requirements (Business)

Updated Operational Readiness Review Requirements

Prospective and existing web-brokers must comply with the following requirements:

Annual data request	• The data request includes 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.

Updated Onboarding Requirements for Prospective Web-brokers

Prospective web-brokers must also comply with the following additional requirements:

- **Pre-approval Website Review**: CMS will review prospective web-brokers' websites to ensure compliance with DE website display requirements and guidance.
- **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. Web-brokers will receive CMS zONE access 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.

- 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
- Additional information related to the web-broker onboarding process is detailed on CCIIO's website at https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/Processes-Becoming-Web-broker.pdf.

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF TECHNOLOGY SOLUTIONS

New Operational Readiness Review Privacy and Security Requirements

New 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 the table to CMS:

Document	Description	Submission Requirements
1. 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 (contact the DE Help Desk for access)

2. Security and Privacy Assessment Report (SAR) – (third-party auditor preferred)	• The report should contain a summary of findings that includes ALL findings from the assessment to include documentation reviews, control testing, scanning, penetration testing, interview(s), etc.
	  • Explain if and how findings are consolidated.
	  • Ensure risk level determination is properly calculated, especially when weaknesses are identified as part of the Center for Internet Security (CIS) Top 20 and/or OWASP Top 10
	• 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.
		• Submit via the secure portal using the SAR template on CMS zONE

Required Privacy and Security Documentation (continued)

Document	Description	Submission Requirements

Security and Privacy Assessment (SAR) – (third-party auditor preferred) (continued)	• Assessment options: The report may be prepared by:
	1. A third-party auditor (recommended); or
	2. Internal staff, provided that:
	  • They have appropriate qualifications to evaluate security and privacy controls. The internal staff should be familiar with National Institutes 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.
	  • They are not involved in the developmental, operational, and/or management chain associated with the system that is the subject of the assessment.
	• Alternatively, the web-broker may reference existing audit results that address some or all of the assessment's requirements, assuming the existing audit results were produced by a third-party auditor or internal staff in conformity with the requirements described above.
	  • If existing audit reports do not address all required elements of the assessment, the remaining elements must be addressed utilizing one of the first two assessment options.
		• Submit via the secure portal using the SAR template on CMS zONE

3. Network Component and 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. • Similar findings can be consolidated.	• Submit via the secure portal

Required Privacy and Security Documentation (continued)

Document	Description	Submission Requirements
4. Plan of Action and Milestones (POA&M)	• Submit a POA&M if its assessor 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.	• Submit via the secure portal using the POA&M template on CMS zONE
5. Non-Exchange Entity System Security and Privacy Plan (NEE SSP) – if requested	• The NEE SSP must include complete and detailed information about the prospective or existing web-broker's implementation specifications of required security and privacy controls.	• Web-brokers are not required to submit the NEE SSP to CMS. However, CMS may request and review the NEE SSP. • If requested to submit, web-brokers must use the NEE SSP template on CMS zONE.

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF TECHNOLOGY SOLUTIONS

Deadlines and Final Approval

Deadlines

Privacy and Security Documentation: Prospective and existing web-brokers must submit the privacy and security documentation on slides 12-14 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.

Operational Readiness Review Requirements (Business): Prospective and existing web-brokers must meet the new operational readiness review requirements on slides 9 and 10 as part of the onboarding or renewal processes, as applicable.

Final Approval - What to Expect

- 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 the privacy and security documents are deemed complete and once the entity has met all other requirements in the guidance.

Information for Web-brokers That are Existing or Prospective EDE Entities

- The NEE SSP, SAR, and POA&M templates referenced in this presentation are largely the same as the templates used for EDE. However, web-brokers seeking to participate in EDE must implement all security and privacy controls documented in the NEE SSP.
- CMS strongly recommends all web-brokers implement all controls listed 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 described in this presentation 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).
  - If a web-broker's assessment submitted for EDE approval did not include all classic DE environments and functionality, the web-broker must conduct an assessment and submit the DE suite of privacy and security documents for the classic DE privacy and security assessment as described.
  - If a web-broker's classic DE environment was included within the bounds of its EDE audit, the web-broker should notify CMS via email. CMS may request additional documentation to verify the EDE audit boundary included the classic DE website and systems.
- 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.

Summary

- Starting January 1, 2020, web-brokers will no longer submit Appendix D in the Web-broker Agreement.
- Instead, prospective and existing web-brokers will be required to submit the required privacy and security documentation (i.e., annual penetration testing, network and component vulnerability scans, as well as the SAR, POA&M, and NEE SSP (if requested) templates). Prospective or Existing EDE Entities may be impacted as noted on the previous slide.

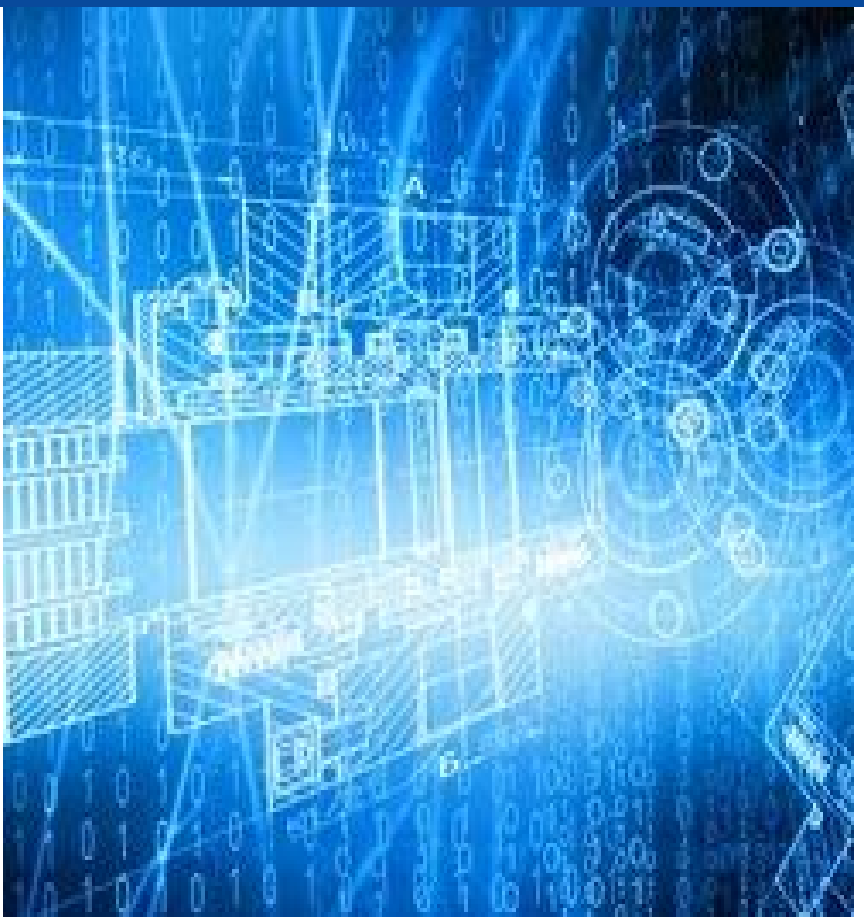
Privacy and Security Documentation Submission Deadlines

Prospective and existing web-brokers must submit the privacy and security documentation as soon as possible during their respective onboarding and renewal 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.

- In addition, starting January 1, 2020, web-brokers are subject to the following new operational readiness review requirements as part of the web-broker onboarding or renewal processes, as applicable:
  - Annual data request
  - Pre-approval website review (prospective web-brokers only)
  - Testing, including renewal testing (if applicable)
  - New timing of execution of the Web-broker Agreement - Prospective web-brokers will build their DE websites and complete technical onboarding prior to receiving a countersigned Web-broker Agreement from CMS.
- **The detailed guidance is available on CCIIO's website:** https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/Guidance-on-Updated-DE-Web-broker-Program-Requirements.pdf

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

Resources



Resources: Web-broker Specific

- *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
- Processes and Guidelines for Becoming a Web-broker in the Federally-facilitated Exchange: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/Processes-Becoming-Web-broker.pdf
- DE Web-broker Public List: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Web-brokers-in-the-Health-Insurance-Marketplace.html
- Additional resources can be found on CCIIO's Web-broker Resources webpage: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Web-brokers-in-the-Health-Insurance-Marketplace.html
- CMS zONE: CMS currently posts all technical information, guidelines, 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 Web-Broker Community (for web-brokers) only.
- CMS currently hosts the Issuer Technical Workgroup (ITWG) webinar weekly on Tuesdays from 3:00 to 4:30 PM ET. The ITWG call is open to all web-brokers and issuers operating on the FFE or SBE-FPs.
- Help Desk:
  - Compliance and assessment-related questions should be sent to the DE Help Desk at directenrollment@cms.hhs.gov
  - Technical issues or questions that concern their technical build or system issues identified in the test or production environment should go to the FEPS Help Desk at CMS_FEPS@cms.hhs.gov
  - Questions related to Hub onboarding for DE should be sent to Hub Help Desk at dsh.support@qssinc.com

Resources: EDE Specific

- 2019/2020 Guidelines for 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 EDE Pathway: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/FAQ-EDE-CY2020.pdf
- List of approved EDE Entities: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/EDE-Approved-Partners.pdf

Closing Remarks