Enhanced Direct Enrollment (EDE): Overview for Federally-facilitated Exchange (FFE) & State-based Exchange using the Federal Platform (SBE-FP) States

October 2, 2019

Center for Consumer Information and Insurance Oversight (CCIIO)

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.

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

HTTPS://WWW.REGTAP.INFO

Webinar Agenda

- Session Guidelines
- Key Dates
- EDE: Overview for FFE & SBE States
- Question & Answer (Q&A) Session
- Closing Remarks

Webinar Audience

- Please be advised that this is not an open press call.
- Members of the press or a media outlet should disconnect the call at this time and contact the Centers for Medicare & Medicaid Services (CMS) Press Office for further information.

Session Guidelines

- This is a 60-minute webinar session.
- Throughout the webinar, you may submit questions via the Q&A Panel.
- We will address questions during the Q&A session at the end of the presentation.
- For questions regarding content or logistics, contact the Registration for Technical Assistance Portal (REGTAP) Registrar at registrar@regtap.info or (800) 257-9520.

Upcoming Key Dates for Plan Year (PY) 2020 QHP Certification

Date	Category	Activity
Tuesday, October 1, 2019	QHP Certification	All Plan Year (PY) 2020 Issuer Testing Begins
Thursday, October 3, 2019	QHP Certification	CMS releases certification notice with the final plan list and countersigned agreements to states

Announcements

Intended Audience and Purpose

- The intended audience for this presentation are Federally Facilitated Exchange (FFE) and State Based Exchange Federal Platform (SBE-FP) states, particularly for those whose issuers are exploring becoming EDE “Upstream Entities.”
- The purpose of this presentation is to provide a high-level overview of the EDE program, EDE oversight, program timelines, and other important considerations for states communicating with issuers interested in seeking approval to participate.
- CMS released the detailed set of guidelines on February 19, 2019: https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Guidelines-for-Third-party-Auditors-EDE-PY19PY20.pdf.
  - EDE Entities already approved to use the EDE pathway or prospective EDE Entities awaiting approval for EDE will need to review the detailed set of updated guidelines.

Agenda

- EDE Introduction
- CMS EDE Oversight
- Security and Privacy Audit
- Questions

EDE Introduction

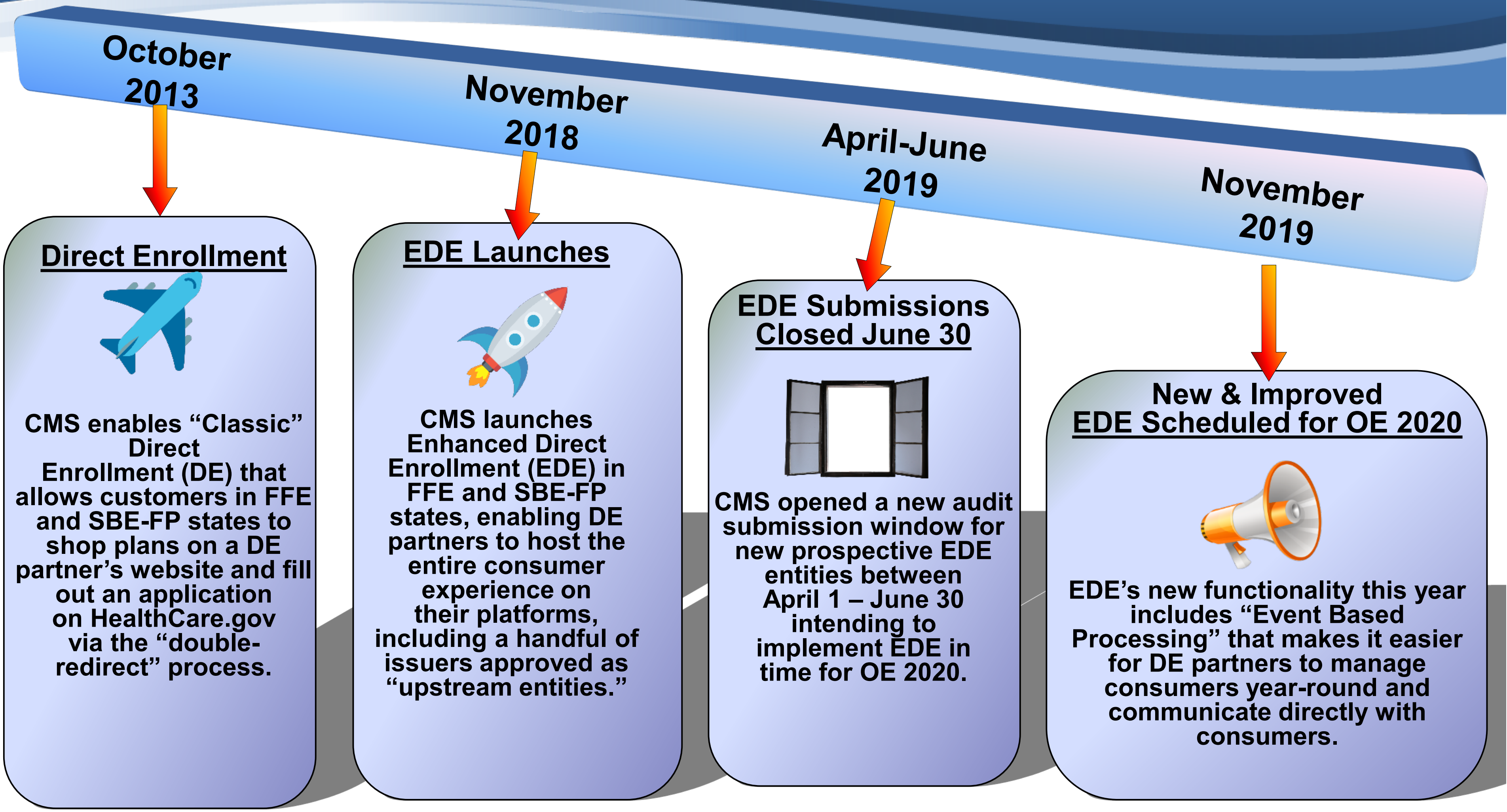
EDE Background

- Enhanced Direct Enrollment (EDE) is an optional program that allows EDE Entities (QHP issuers, web-brokers and technology providers) to host an application for coverage on their own websites for coverage offered on the FFEs and SBE-FPs (also known as the Marketplace).
- EDE allows consumers to complete all steps in the eligibility and enrollment process directly on the private EDE Entity's website without ever having to visit HealthCare.gov. The new process expands the use of application programming interfaces (APIs) to transfer data between the FFE and approved partner websites and agents and brokers.
- This new functionality enables private EDE Entities to innovate new enrollment processes to improve the consumer experience in shopping for, applying for, and enrolling in Exchange coverage.
- CMS launched the EDE program in 2018 and the first EDE Entities were approved during the plan year (PY) 2019 Open Enrollment Period (OEP).

ℹ

- For a summary of the EDE program, please refer to the Frequently Asked Questions (FAQs) for Enhanced Direct Enrollment.
- For a summary of the EDE timeline for calendar year 2019, please refer to the FAQ: Enhanced Direct Enrollment Calendar Year 2019 Timeline.
- For a summary of the EDE timeline for calendar year 2020, please refer to the FAQ: Enhanced Direct Enrollment Calendar Year 2020 Timeline.

The Direct Enrollment (DE) Journey So Far



October 2013

Direct Enrollment

CMS enables “Classic” Direct Enrollment (DE) that allows customers in FFE and SBE-FP states to shop plans on a DE partner’s website and fill out an application on HealthCare.gov via the “double-redirect” process.

November 2018

EDE Launches

CMS launches Enhanced Direct Enrollment (EDE) in FFE and SBE-FP states, enabling DE partners to host the entire consumer experience on their platforms, including a handful of issuers approved as “upstream entities.”

April-June 2019

EDE Submissions Closed June 30

CMS opened a new audit submission window for new prospective EDE entities between April 1 – June 30 intending to implement EDE in time for OE 2020.

November 2019

New & Improved EDE Scheduled for OE 2020

EDE’s new functionality this year includes “Event Based Processing” that makes it easier for DE partners to manage consumers year-round and communicate directly with consumers.

Why EDE?

Bring More Private Sector Innovation to the Exchanges

- Encourage **innovation in the private sector** to experiment with how best to enroll consumers.
- Provide DE partners with data that helps them more fully **manage their clients' coverage**.
- Create Exchange stability through broader and expanded **alternative enrollment platforms**.

Improve the Consumer Experience

- Enable DE partners to provide a **unique and tailored user experience** to their consumers.
- Enable DE partners to host the **entire consumer application** on their platforms.
- Enable consumers to **interact with DE partners directly** via their platforms.

Enable Issuers & Partners to Directly Manage their Customers

- Help DE partners to initiate and fully **maintain customer relationships year-round**.
- Make it easy for DE partners to provide **post-enrollment services** directly to their enrollees.
- Provide **real-time data tools** that help DE partners retain their customers.

Key Differences between EDE & "Classic" DE

Functionality	Classic DE	EDE
• Consumers start their QHP shopping experience by visiting the DE partner site.	X	X
• Consumers must visit HealthCare.gov at key points during the application process in order to complete their enrollment.	X	
• Consumers stay on the DE partner site throughout the entire application and enrollment process.		X
• DE partners can customize the consumer application (within guardrails).		X
• Consumers can upload documentation to resolve SVIs/DMIs on the DE partner site.		X
• Consumers can view the status of their policy, SVIs, and DMIs on the DE partner site.		X
• Consumers can download notices directly from the DE partner site.		X
• Consumers can always return to the DE partner site for changes in circumstances and Special Enrollment Periods (SEPs) if supported by the application phase.		X
• Partners own and manage all communications directly with the consumer (rather than CMS/HealthCare.gov) wherever feasible.		X

How it Works: The Suite of EDE API's

EDE partners integrate their systems with CMS' systems through software-to-software information exchange interfaces, which are known as **application program interfaces (APIs).**

Class of API	Functionality
Eligibility APIs	• Enable EDE partners to create, update, submit, delete or view a consumer's application (all with consumer consent).
Enrollment APIs	• Provide EDE partners with the capabilities to retrieve and modify enrollment data in real time. • Allow EDE partners to submit enrollments to the Exchange.
Customer Service-APIs	• Check data-matching issue (DMI) and/or Special Enrollment Period (SEP) verification issue (SVI) status. • Store the ID proofing record and establish permission for an EDE partner to perform work on behalf of the consumer. • Upload documents for DMI/SVI adjudication. • Retrieve Exchange notices. • Redirect consumers to issuer sites for binder payments. • Retrieve consumer business events for purposes of consumer messaging.

Bottom line: EDE is much more than hosting the consumer application. EDE partners leverage the APIs above to manage the entire end-to-end consumer experience and account management.

EDE Implementation: 3 Successive Application Builds (Each EDE Partner Selects Initial Starting Phase)

Phase 1: Simplified Application Build

- Support consumer scenarios currently provided by the simplified application, also referred to by issuers and partners as “Application 3.0.”
- The minimum level of support required of any EDE partner when they start.

Phase 2: Expanded Application

- Support consumer scenarios from Phase 1.
- In addition, support an expanded (but not infinite) list of consumer support scenarios (including: full-time students, pregnant application members, naturalized US citizens, and step children).

Phase 3: Complete Application

- Support all consumer scenarios (aka “the kitchen sink”).
- Examples of additional scenarios include application members living at different addresses, married couples filing separate tax returns, and more.

In all phases, the EDE partner provides the full EDE API Suite (including eligibility, enrollment and customer service APIs.)

Partners Live with EDE as of October 2, 2019

Entity Name	Primary Partner	Upstream Entity (Issuer)	Current Phase
HealthSherpa	**X**		**2**
• Aspirus Arise Health Plan of WI		X	
• Blue Cross Blue Shield of NC		X	
• Cigna		X	
• Dean Health Plan		X	
• MercyCare Health Plans		X	
• Molina Healthcare		X	
• Oscar Insurance Company		X	
• Security Health Plan of WI		X	
Stride Health	**X**		**1**
Guidewell Connect	**X**		**2**
• Florida Blue		X	
GetInsured	**X**		**3**
Softheon	**X**		**3**

We currently anticipate several additional issuers signing up to become "Upstream Entities" to leverage an approved EDE Primary partner's platform by the launch of Open Enrollment this fall.

CMS EDE Oversight

EDE Oversight

- To pursue EDE, prospective EDE Entities must build their EDE environments and security programs. Then, prospective EDE Entities must have one (1) or more third parties conduct audits consisting of two (2) parts (a Business Requirements Audit and a Security and Privacy Audit). The audits must be submitted to CMS within the submission windows established by CMS.
- The primary audit submission window for prospective EDE Entities interested in implementing EDE in calendar year 2020 for PY 2020 and PY 2021 is March 1, 2020 to June 30, 2020.
- For more information on basic EDE program requirements and details, refer to the updated EDE guidelines that were released in February 2019: https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Guidelines-for-Third-party-Auditors-EDE-PY19PY20.pdf.

Types of EDE Entities (Options to Participate)

- Prospective EDE Entities have two (2) main options to consider in determining how and to what extent to pursue participation in EDE during calendar year 2019:
  - A primary EDE Entity is an entity that develops, designs, and hosts its own EDE environment for its own use or for use by others.
    - Prospective EDE Entities that wish to participate in EDE independent of another entity must first be approved to participate in DE as an issuer or web-broker.
  - An upstream EDE Entity is an entity that will use an EDE environment provided by a primary EDE Entity. Upstream EDE Entity models include:
    - Issuer upstream EDE Entities.
    - Non-issuer upstream EDE Entities engaged in "hybrid" arrangements, and
    - Use of a white-label primary EDE Entity's environment by a non-issuer.

    Note: All upstream EDE Entities must have a legal relationship with a primary EDE Entity.
- The list of EDE Entities that are approved to use the EDE pathway is available here
  - This list is updated frequently, but it may not immediately reflect EDE Entities most recently approved to use the EDE pathway.

Non-issuer Users of a Primary EDE Entity's EDE Environment

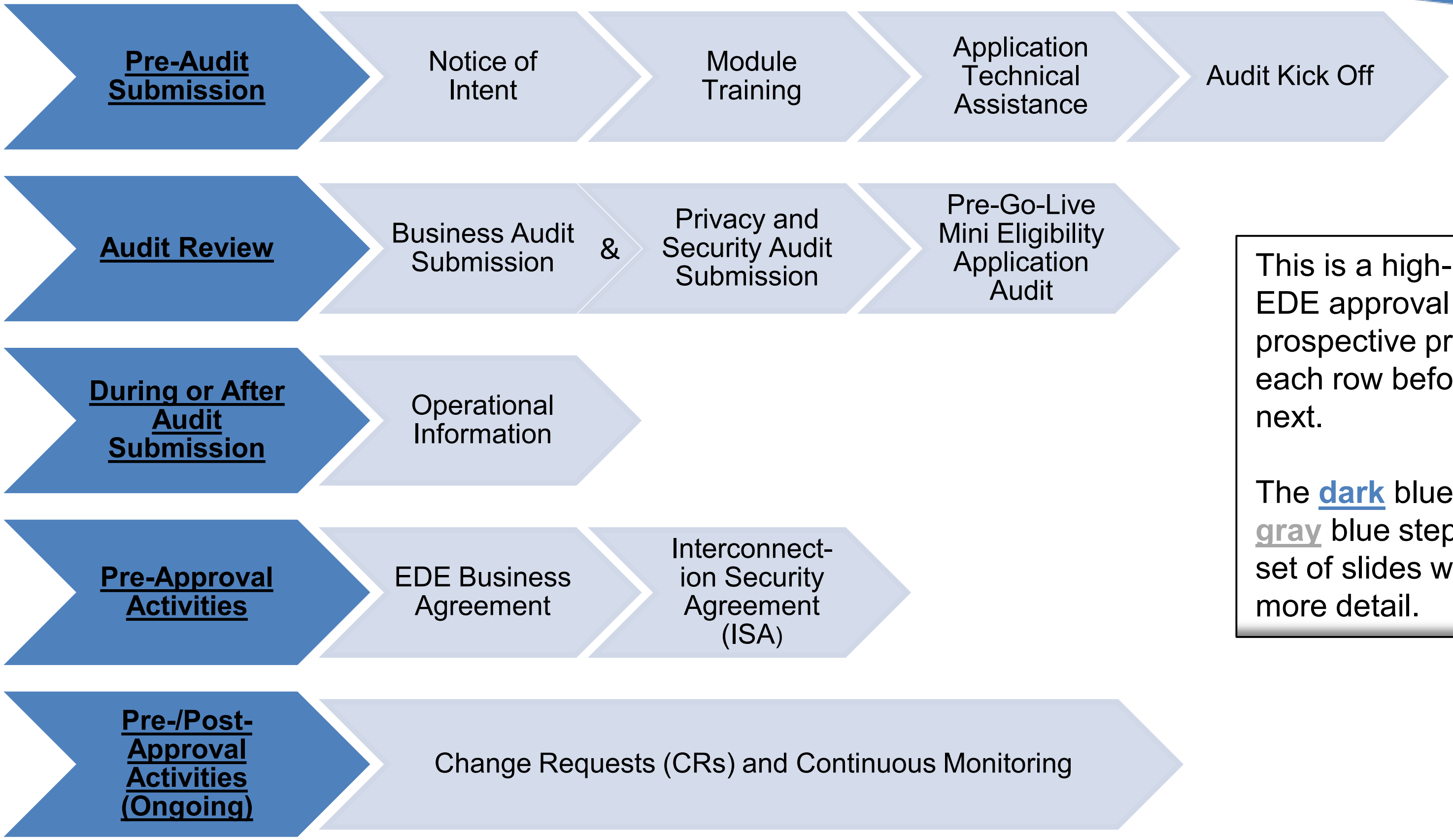
Model 1: White-Label Non-Issuer Users

- Limited to "minor branding changes only" to the primary EDE Entity's EDE environment as defined in the EDE Guidelines
- May be utilized by downstream and delegated agents and brokers
- Users within this classification have added no functionality or systems that constitute part of the overall EDE end-user experience
- Not required to maintain a unique partner ID, sign the EDE Business Agreement, or submit an audit

Model 2: Hybrid, Non-Issuer Upstream EDE Entities

- Adds functionality or systems to the overall EDE end-user experience
  - For example, utilization of redirects between a primary EDE Entity's EDE website and a web-broker's classic DE website to constitute the overall EDE end-user experience
- Required to maintain a unique partner ID, sign the EDE Business Agreement, and submit a modified version of an EDE privacy and security audit

EDE Oversight Process – Summary



Pre-Audit Submission: Notice of Intent → Module Training → Application Technical Assistance → Audit Kick Off

Audit Review: Business Audit Submission & Privacy and Security Audit Submission → Pre-Go-Live Mini Eligibility Application Audit

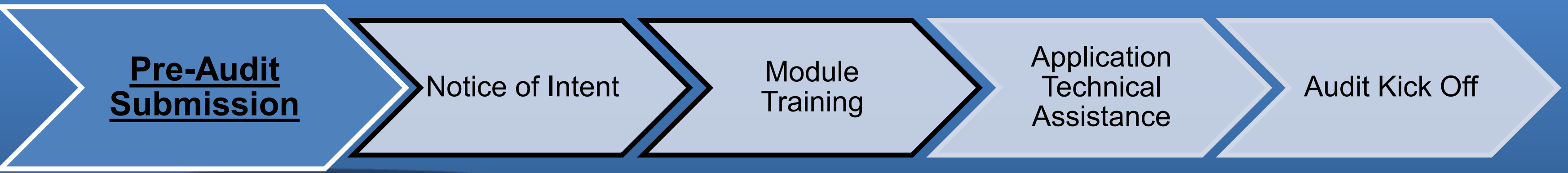
During or After Audit Submission: Operational Information

Pre-Approval Activities: EDE Business Agreement → Interconnect-ion Security Agreement (ISA)

Pre-/Post-Approval Activities (Ongoing): Change Requests (CRs) and Continuous Monitoring

This is a high-level summary of the EDE approval process. In general, prospective primary entities complete each row before progressing to the next.

The **dark** blue chevrons summarize the gray blue steps in each row. The next set of slides will describe each row in more detail.



Notice of Intent

- If a prospective EDE Entity intends to submit its audit during the March 1, 2020 to June 30, 2020 submission window, it must send its notice of intent to CMS.

Module Training

- The Auditor(s) selected by the prospective EDE Entity and representative(s) from the prospective EDE Entity are required to take CMS-mandated trainings that target the main components of EDE and EDE oversight.
  - The training is a self-paced computer-based training (CBT) and provides information about compliance, EDE technical requirements, privacy and security, and reporting requirements.
  - REGTAP can be accessed at the following link: https://www.regtap.info/.

Business Requirements Auditor Training Requirement

- An Auditor who will be completing the business requirements audit must complete the following training modules before initiating that audit:
  - EDE Regulatory/Compliance Standards,
  - EDE Application UI Overview,
  - EDE ORR and CMS Reporting Requirements,
  - EDE User Interface (UI) Services, and
  - Other potential modules to be defined by CMS.

Privacy and Security Auditor Training Requirement

- An Auditor who will be completing the privacy and security audit must complete the following training modules before initiating the audit:
  - EDE Regulatory/Compliance Standards,
  - EDE Privacy/Security Standards, and
  - Other potential modules to be defined by CMS.

Prospective EDE Entity Training Requirement

- Representative(s) from the primary prospective EDE Entity must take all training modules.
- CMS encourages representatives from upstream entities to take all trainings as well.

Application Technical Assistance

- Prior to conducting and submitting an audit, a prospective EDE Entity can request feedback from CMS on its planned application UI build to:
  - Answer clarifying questions about application requirements,
  - Help mitigate the risk that CMS identifies compliance issues later, and
  - Ask specific questions related to UI development such as policy guidance, application requirements and flexibilities, technical design, and high-level application requirements and flow.
- Regardless of whether a prospective EDE Entity requests feedback from CMS, all prospective EDE Entities must provide testing environment credentials for possible additional testing.

Audit Kick Off

- The Entity must notify CMS before its Auditor begins its audit (at least one (1) to two (2) weeks prior). CMS will schedule a kickoff call before the audit is initiated to answer questions, ensure expectations are clear, and ensure the Auditor and prospective EDE Entity are using the correct audit documents. Additional check-in calls may be scheduled. CMS also requires two (2) documents:
  - □ The Entity's privacy and security Auditor must complete the Security and Privacy Controls Assessment Test Plan (SAP). The SAP will contain a high-level description of the critical items that the Auditor must test. This must be submitted to CMS for review prior to conducting the privacy and security audit.
  - □ The Entity must submit a copy of the signed agreement or contract between the Auditor(s) and prospective primary EDE Entity.

Note on Auditor Independence:

- An independent third-party Auditor is independent if there is no perceived or actual conflict of interest involving the developmental, operational, and/or management chain associated with the system and the determination of effectiveness (e.g., security and privacy control effectiveness).
- The Auditor's role is to provide an independent assessment of the compliance of the EDE Entity's EDE environment and to maintain the integrity of the audit process.

Overview of Business Requirements Audit

- An Auditor will complete a business requirements audit to ensure the prospective EDE Entity has complied with applicable requirements as defined in CMS's EDE implementation guidance.
- The business requirements audit focuses on, but is not limited to, the following requirements:

❑ Identity proofing of consumers and agents/brokers

❑ Eligibility application user interface (UI) (e.g., accuracy, correct implementation, and validation)

❑ Communications (e.g., post-eligibility communications and accurate communications about the Exchange and consumer communications

❑ Documentation of interactions with consumer applications or the Exchange

❑ Eligibility results testing and Standalone Eligibility Service (SES) testing

❑ Functional integration of APIs

❑ Section 508 compliance

❑ Non-English language versions of relevant audit components

- Business Audit Documentation: A prospective EDE Entity must submit the Business Requirements Audit Report Template, four (4) applicable toolkits completed by its Auditor, and supplemental documentation (e.g., screenshots). The toolkits target the major components of EDE environments, such as integrating APIs correctly, generating the correct eligibility results for consumers, and sufficiently communicating with consumers.

Audit Submission **Completeness** Review

- CMS reviews each audit submission for completeness (e.g., test cases produced correct eligibility results, the Auditor completed each document, etc.).
- CMS will not accept incomplete audits. In this case, the Auditor must complete incomplete audits in accordance with the CMS-defined standards.

Audit Submission **Compliance** Review

- Once the submission is deemed complete, CMS reviews the submission for compliance with the business and privacy and security requirements.
  - For the business audit submission, all high-risk issues must be resolved before the mini audit. The Entity may resolve remaining low-risk ORR findings within 30 days of approval to go live.
- For the privacy and security audit submission, the Entity works with CMS until it has reached the necessary security posture.

Note on Timing and Best Practices:

- Once an audit is deemed complete, resubmissions may stem from compliance findings in the audit submission and resubmissions, and issues and findings in the EDE environment and eligibility application. Therefore, the quality of the EDE environment, the quality of documentation submitted to CMS, and the quality and timeliness of resubmissions affect the time it takes to progress through the approval process.

Pre-Go-Live Mini Eligibility Application Audit (Mini Audit)

- When CMS confirms that a prospective EDE Entity's application UI complies with application guidelines and requirements based on review of its Auditor's assessment and any feedback from the CMS technical assistance team, CMS will conduct a mini audit of the Entity's application prior to final approval of the Entity's EDE environment.
- CMS will review any compliance issues identified during the mini audit and provide written feedback to the prospective EDE Entity of changes that the prospective EDE Entity will be required to make prior to final approval. The prospective EDE Entity must submit proof that it implemented the required changes to CMS. CMS will subsequently provide further feedback or approval.
- The mini audit is not intended to replicate an Auditor's review of a prospective EDE Entity's EDE environment; the mini audit focuses on reviewing a subset of eligibility scenarios for compliance, including application elements such as question and answer text.

Note on Testing Environment Requirements to Help Ensure an Accurate Audit:
The prospective EDE Entity will be required to provide CMS with a set of credentials that CMS can use to access the Entity's testing environment. The prospective EDE Entity must ensure that the testing credentials are valid and that all APIs and components of its EDE implementation in its testing environment, including the RIDP services, are accessible for the duration of the mini audit.

Operational Information

- Organizations participating as a prospective primary EDE Entity must submit the documentation listed below (upstream EDE Entities submit a subset of these documents):

Privacy Questionnaire

- Asks questions related to Entity websites and what information is collected, how that information is used, and which tracking technologies are utilized in order to assess any privacy impact to consumers

Entity's website privacy policy statement(s) and Terms of Service

- Includes the URL and text of each privacy policy statement displayed on the website, and the website's Terms of Service

Primary EDE Entity Audit Submission Questionnaire

- Collects operational information (e.g., service areas)

ISA Appendix B – "Data Sharing and Connection Information.doc"

- Captures information about the data connections, functionality, and systems between a primary EDE Entity and its upstream EDE Entities
  - For example, entities must describe the information transmitted between primary and upstream entities (e.g., personally identifiable information [PII] data elements, enrollment information, eligibility information, 834s, etc.) and the privacy and security protections applied to such data

EDE Business Agreement

- Primary and upstream EDE Entities must submit the EDE Business Agreement to use the EDE pathway.
- CMS will countersign the EDE Business Agreement after CMS has reviewed and approved the business requirements audit and the privacy and security audit.

Interconnection Security Agreement (ISA)

- A prospective primary EDE Entity must submit the ISA to use the EDE pathway.
- CMS will countersign the ISA after CMS has reviewed and approved the business requirements audit and privacy and security audit.

Change Requests (CRs) and Continuous Monitoring

Change Requests (CRs)

- CMS periodically releases updates to EDE program requirements in the form of CMS-initiated CRs. CMS may require EDE Entities to implement new or updated EDE requirements. These required revisions will be considered CMS-initiated CRs.
- If an EDE Entity wishes to make changes to its EDE environment that was audited by a third-party Auditor and approved by CMS for use in PY 2019, the EDE Entity must follow the process defined by CMS.

Continuous Monitoring

- Continuous Monitoring of Compliance with Business Requirements
  - After CMS issues final approval, it will conduct periodic, post-go-live mini audits. If CMS identifies compliance issues during these mini audits, CMS may immediately suspend the EDE Entity's EDE connection until the Entity has addressed any identified compliance issues to CMS' satisfaction.
  - If CMS identifies any compliance issues likely to affect a consumer's eligibility application or results during a post-go-live mini audit, CMS may require the EDE Entity to contact consumers to collect the appropriate eligibility information and resubmit applications that may have been affected by the compliance issues.
  - CMS may, at its discretion, conduct mini audits following any post-approval changes to an EDE Entity's EDE environment.
- Continuous Monitoring of Compliance with Privacy and Security Requirements
  - This process will be discussed later in the presentation.

Publicly Available EDE Resources for Prospective EDE Entities That Are Not DE Entities

Resource	Description	Link
Guidelines for Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements	Updated set of EDE guidelines published in February 2019	https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Guidelines-for-Third-party-Auditors-EDE-PY19PY20.pdf
Processes and Guidelines for Becoming a Web-broker in the Federally-facilitated Exchanges	Presentation reviews the registration process and operational requirements for web-brokers to operate in the FFEs and SBE-FPs	https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/Processes-Becoming-Web-broker.pdf
FAQ: Enhanced Direct Enrollment Calendar Year 2019 Timeline	Overview of requirements and submission timelines for prospective EDE Entities that plan to apply to use the EDE pathway in calendar year 2019	https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/FAQ-EDE-CY2019.pdf
FAQ: Enhanced Direct Enrollment Calendar Year 2020 Timeline	Overview of requirements and submission timelines for prospective EDE Entities that plan to apply to use the EDE pathway in calendar year 2020	https://www.cms.gov/CCIIO/Resources/Fact-Sheets-and-FAQs/Downloads/FAQ-EDE-CY2020.pdf
FAQs Regarding EDE Participation Requirements for Non-Issuer Users of a Primary Entity's EDE Environment	This document contains FAQs related to more specific requirements for two models for EDE participation	
FFE and FF-SHOP Enrollment Manual	Operational policy and guidance on key topics related to eligibility and enrollment activities within the FFEs and FF-SHOPs, as well as within the SBEs-FP	https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Enrollment-Manual-062618.pdf
EDE computer-based-trainings (CBTs) on REGTAP	Initial set of EDE trainings; CMS may release updated required trainings. A REGTAP account is required to view this material.	https://www.regtap.info/DirectEnrollment.php

Security and Privacy Audit

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Overview of Security and Privacy Audit

- An EDE Entity must implement security and privacy controls, as well as meet other security and privacy standards, to protect the confidentiality, integrity, and availability of the information collected, used, disclosed, and/or retained by the EDE Entity as defined by CMS in the Interconnection Security Agreement (ISA).
- The EDE Entity and its independent third-party Auditor will work together to develop the Security and Privacy Controls Assessment Test Plan (SAP). This SAP must be submitted to CMS for review prior to the assessment.
- Once the EDE Entity has **fully completed** and implemented its System Security and Privacy Plan (SSP), and no issues arise from CMS's review of the SAP, only then should the Auditor begin the security and privacy audit.

The Auditor should not begin the assessment if the SSP is incomplete.

Auditor Experience

- CMS requires that the EDE Entity's Auditor possess a combination of security and privacy experience and relevant auditing certifications.
- Examples of acceptable security and privacy experience include, but are not limited to:
  - Federal Information Security Management Act (FISMA) experience;
  - Federal Risk and Authorization Management Program (FedRAMP)-certified third-party assessment organization;
  - Statement on Standards for Attestation Engagements (SSAE) 16 experience;
  - Reviewing compliance with NIST SP 800-39; NIST SP 800-30 Rev. 1; NIST SP 800-37 Rev. 2; NIST SP 800-53 Rev. 4; and
  - Reviewing compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule standards.
- Examples of relevant auditing certifications include, but are not limited to:
  - Certified Information Privacy Professional (CIPP), Certified Information Privacy Professional/Government (CIPP/G);
  - Certified Information Systems Security Professional (CISSP);
  - Fellow of Information Privacy (FIP);
  - HealthCare Information Security and Privacy Practitioner (HCISPP);
  - Certified Internal Auditor (CIA), Certification in Risk Management Assurance (CRMA);
  - Certified Information Systems Auditor (CISA); or
  - Certified Government Auditing Professional (CGAP).

CMS strongly recommends that the EDE Entity select an Auditor from the FedRAMP-certified third-party assessment organization (3PAO) list.

Submission Process Considerations: Having a Complete Security and Privacy Audit

- Complete Audit: The prospective EDE Entity must provide a complete security and privacy audit that meets the following minimum criteria:
  - Security and Privacy Controls Assessment Test Plan (SAP)
    - Note: This is completed and submitted to CMS for review PRIOR to the audit and is not part of the audit submission.
  - Security and Privacy Assessment Report (SAR)
  - Plan of Action and Milestones (POA&M)
  - Vulnerability Scans
  - Interconnection Security Agreement (ISA)
  - Information Security and Privacy Continuous Monitoring (ISCM) activities
    - Note: This is not part of the initial audit, but is part of subsequent audits per the ISCM plan and plan for reauthorization to connect.
- Incomplete Audit: CMS will not accept an incomplete or partial audit. Prospective EDE Entities with incomplete audits must resubmit a complete audit for CMS review.

Submission Process Considerations: Having a Complete Security and Privacy Audit (Continued)

Document	Minimum Requirements for a Complete Audit
Security and Privacy Controls Assessment Test Plan (SAP)	▪ The SAP describes the Auditor's scope and methodology of the assessment. ▪ The SAP includes an attestation of the Auditor's independence. ▪ The SAP must be completed by the Auditor and submitted to CMS for review, prior to conducting the security and privacy controls assessment (SCA).
Security and Privacy Assessment Report (SAR)	▪ The SAR is not a living document; findings should not be added/removed from the SAR unless CMS's initial review of the final draft discovers deficiencies or inaccuracies that need to be addressed. ▪ The SAR should contain a summary of findings that includes ALL findings from the assessment, including documentation reviews, control testing, scanning, penetration testing, and interview(s). ▪ 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 Open Web Application Security Project (OWASP) Top 10. ▪ Only one (1) final SAR should be submitted to CMS. Once that SAR has been submitted and CMS has no additional comments or edits on the SAR, the prospective EDE Entity should not submit additional SARs.
Plan of Action and Milestones (POA&M)	▪ 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. ▪ Monthly reviews and updates are required until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities described in the EDE SSP controls CA-5 and CA-7. Prospective EDE Entities 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.

Submission Process Considerations: Having a Complete Security and Privacy Audit (Continued)

Document	Minimum Requirements for a Complete Audit
Monthly Vulnerability Scans	▪ The EDE Entity must conduct monthly vulnerability scans of its IT system(s). ▪ The EDE Entity must submit the most recent three (3) months of vulnerability scans to CMS for review during ISCM activities. ▪ All findings from vulnerability scans are expected to be consolidated in the monthly POA&M. ▪ Similar findings can be consolidated.
Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide	▪ This ISCM Guide describes CMS's strategy for instructing EDE Entities in following the initial approval of the Request to Connect (RTC). The ISCM Guide conveys the minimum requirements for EDE Entities that implement an ISCM program for their systems and to maintain ongoing CMS RTC approval. ▪ ISCM describes the monthly, quarterly, and annual reporting summaries. ▪ ISCM describes the security and privacy controls action frequencies. ▪ ISCM describes the subset of security and privacy core controls that must be tested annually.

Information Security and Privacy Continuous Monitoring (ISCM)

- Approved EDE Entities must adhere to the continuous monitoring reporting requirements in the ISCM Strategy Guide, which includes the completion of an annual assessment of security and privacy controls described in the ISCM.
- ISCM provides a mechanism for the EDE Entity to identify and respond to new vulnerabilities, evolving threats, and constantly changing enterprise architecture and operational environment, such as changes in the hardware or software, as well as data creation, collection, disclosure, access, maintenance, storage and use.
- The ISCM Strategy Guide provides the minimum requirements for EDE Entities to implement an ISCM program for their systems and to maintain ongoing CMS authorization and approval.
- Ongoing assessment and authorization provides CMS a method of detecting changes to the security and privacy posture of an EDE Entity's IT system that are essential to making well-informed risk-based decisions.

ISCM Requirements

- Monthly EDE Entity activities:
  - POA&M updates
  - Vulnerability scans
- Quarterly EDE Entity activities:
  - Continuous monitoring reports that follow the reporting requirements identified in EDE SSP CA-7 Continuous Monitoring Control
- Annual EDE Entity submission to CMS include:
  - Annual Security and Privacy Assessment Report (SAR) of the CMS-defined subset of security and privacy core controls
  - Annual penetration test results during reauthorization
  - Annual System Security and Privacy Plan (SSP) updates
  - Most recent three (3) months of vulnerability scans
  - POA&M updates
    - Monthly submissions to CMS until all significant or major findings are resolved
    - Quarterly POA&M submissions are required as part of the ISCM activities, thereafter

ISCM Change Control

- Configuration management and change control processes help maintain a secure baseline configuration of the EDE Entity's architecture. Routine day-to-day changes are managed through the EDE Entity's change management process described in its Configuration Management Plan.
- At a minimum, the EDE change management process should include the following activities:
  - Determine the nature of change, which includes, but is not limited to:
    - Supporting software changes or version upgrades;
    - Adding services that modify the infrastructure;
    - Modifying the connection to the CMS Data Services Hub;
    - Responding to changes in the business process flow;
    - Handling Personally Identifiable Information (PII) data creation, collection, disclosure, access, maintenance, storage, and use;
    - Adding or modifying applications supporting Exchange functions that may impact security and privacy;
    - Adopting changes in Commercial Off-the-Shelf (COTS) software;
    - Adapting to hardware or infrastructure changes, such as deployment of cloud technology; and
    - Changing operations at the processing site or outsourcing of data center operations.
  - Complete a security impact analysis.
  - Notifying CMS: The EDE Entity completes the System Change Notification Form (CN) Form and submits to CMS.
- There are many factors that could make it difficult to establish specific thresholds for a significant change determination. Therefore, CMS recommends, as a best practice, that the EDE Entity involve the CMS Information System Security Officer (ISSO) in discussions related to any future changes to the system.

Common Controls

- All EDE Entities (primary EDE Entities and upstream EDE Entities) are held to the same set of security and privacy requirements that are documented in the EDE SSP. CMS requires written confirmation from both the primary EDE Entity and upstream EDE Entity to allow a connection to CMS for an upstream entity.
- **Common Controls** are security or privacy controls whose implementation results in a security or privacy capability that is inheritable by multiple information systems being served by the primary EDE Entity. Upstream EDE Entities should leverage the common controls identified by the primary EDE Entity.
- **Security Control Inheritance** defines a situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application (i.e., entities either internal or external to the organization where the system or application resides).
- **Hybrid Control:** It is possible for an information system to inherit just part of a control from a primary EDE Entity, with the remainder of the control provided by the upstream EDE Entity. In this situation, both the primary EDE Entity and the upstream EDE Entity have a shared responsibility of implementing the full control objectives and implementation standards.
- Responsibility for implementing the following -1 controls (policies and procedures) cannot be inherited and must be described in some way by the upstream EDE Entity.
  - AC-1, Access Control
  - AT-1, Awareness and Training
  - CA-1, Security Assessment and Authorization
  - CP-1, Contingency Planning
  - IR-1, Incident Response
  - PS-1, Personnel Security
- For an EDE Entity to inherit a particular security or privacy control implemented by the primary EDE Entity, the following should be true:
  - The primary EDE Entity has designated the control as inheritable by documenting in the EDE SSP implementation description “inheritable.”
  - The primary EDE Entity has received RTC approval from CMS and evidence that the control is in fact operational with no major security weakness findings.

Additional Resources

- 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
- 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
- FAQ: Enhanced Direct Enrollment Calendar Year 2019 Timeline: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/FAQ-EDE-CY2019.pdf
- FFE and FF-SHOP Enrollment Manual: https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Enrollment-Manual-062618.pdf
- List of approved EDE Entities (see “Enhanced Direct Enrollment Approved Partners”): 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
- 2019 Letter to Issuers: https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/2019-Letter-to-Issuers.pdf
- CMS website for issuers seeking certification to participate in the FFEs: https://www.qhpcertification.cms.gov/s/QHP
- CMS zONE:
  - CMS currently posts all technical information, guidelines, audit resources, and other documentation on the CMS zONE EDE Documents and Materials webpage at the following link: https://zone.cms.gov/document/enhanced-direct-enrollment-ede-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.
- Help Desk Support:
  - Compliance and audit-related questions should be sent to the DE Help Desk at directenrollment@cms.hhs.gov
  - Technical issues or questions that concern 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

Live Q&A

Questions

Please help us provide an accurate response by identifying your State when asking a question.

<u>To submit or withdraw questions by phone:</u>

- **To submit a question, dial ‘star(*) pound(#)’ on your phone’s keypad.**
- **To withdraw a question, dial ‘star(*) pound(#)’ on your phone’s keypad.**

<u>To submit questions by webinar:</u>

- **Type your question in the text box under the ‘Q&A’ tab and click ‘Send.’**

If you are not able to ask your question during today’s session, or if your question is best answered by subject matter experts (SMEs) outside Plan Management (PM), you may submit it via CMS_FEPS@cms.hhs.gov with the subject line “State Question.”

State Regulators Webinar Session Survey

- CMS welcomes your feedback regarding this webinar series and values any suggestions that will allow us to enhance this experience for you.
- Shortly after this call, we will send a link to you for a convenient way to submit any ideas or suggestions you wish to provide that you believe would be valuable during these sessions.
- Please take time to complete the survey and provide CMS with any feedback.

Closing Remarks