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

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

May 8, 2019

Updated May 8, 2019: This document has been updated since it was originally posted on January 28, 2019. This updated version replaces the original document.

Frequently Asked Questions (FAQs) Regarding Participation Requirements for Enhanced Direct Enrollment (EDE) Entities Serving Consumers in States with Federally-facilitated Exchanges (FFEs)

The following FAQs detail the requirements and submission timeline for prospective EDE Entities that plan to use the EDE pathway in calendar year 2019 for plan years (PYs) 2019 and 2020 to offer and enroll consumers in qualified health plans (QHPs) through the FFEs and State-based Exchanges on the Federal Platform (SBE-FPs).

1. When can prospective EDE Entities pursue EDE for calendar year 2019?

Centers for Medicare & Medicaid Services (CMS) is continuing to implement EDE, an optional program allowing EDE Entities (QHP issuers and web-brokers may seek to participate in EDE) in the FFEs and SBE-FPs (also known as the Marketplace) to host an application for Marketplace coverage on their own websites. For a summary of the EDE program, please refer to the Frequently Asked Questions (FAQs) for Enhanced Direct Enrollment. For more information on basic EDE program requirements and details, refer to the Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements (Guidelines).

To pursue EDE, prospective EDE Entities must build their EDE environments and submit audits consisting of two parts (a Business Requirements Audit and a Privacy and Security Audit) within the submission windows established by CMS.

The primary audit submission window for prospective EDE Entities interested in implementing EDE in calendar year 2019 for PY 2019 and 2020 is April 1, 2019 to June 30, 2019.[1] CMS will not accept audits outside of this submission window. There is no guarantee that every prospective EDE Entity that submits a complete audit in the submission window will receive approval unless and until the Entity meets all program requirements. CMS will release future guidance about the next annual audit submission window after the PY 2020 open enrollment period (2020 OEP).

[1] A preliminary audit submission window was in effect from December 15, 2018 to January 31, 2019 for those prospective EDE Entities that had substantially completed development of their EDE environments and their related audits in calendar year 2018.

Note: If a prospective EDE Entity submits an audit and resubmits it before hearing from CMS about its original submission, CMS will only consider the date of the latest submission for purposes of determining review priority. CMS will conduct an initial, high-level review of each audit to evaluate the quality and completeness of the audit.

April 1, 2019 to June 30, 2019 Audit Submission Window and Notice of Intent (Updated)

If a prospective EDE Entity intends to submit its audit during the April 1, 2019 to June 30, 2019 submission window, it must send its notice of intent to directenrollment@cms.hhs.gov by February 28, 2019. Once the prospective EDE Entity has a confirmed Auditor(s) who will complete its audit(s), the Entity must notify CMS that it intends to use the EDE pathway for PY 2019 and PY 2020 prior to initiating the audit. Unlike last year, only prospective primary EDE Entities (defined below) must submit a notice of intent informing CMS that they are developing an EDE environment; Prospective upstream EDE Entities that will rely on a primary EDE Entity's pathway should notify CMS of their intent to participate in EDE when or after their prospective primary EDE Entity submits its audit.[2] The subject line of a notice of intent email must read "Enhanced DE: Intent" and the information below must be included in the body of the email:

- Prospective EDE Entity Name;
- Auditor Name(s) and Contact Information (Business Requirements and Privacy and Security, if different);
- EDE Phase (1, 2, or 3);
- Prospective EDE Entity Primary Point of Contact (POC) name, email, and phone number;
- Prospective EDE Entity Technical POC name, email, and phone number;
- Prospective EDE Entity Emergency POC name, email, and phone number; and
- CMS-issued Hub Partner ID.

CMS will conduct an initial, high-level review of all audit submissions in the order they are received. If a prospective EDE Entity submits an incomplete audit, CMS will communicate the missing elements to the Entity based on the initial high-level review, and the audit will be pulled from the review queue. Once the prospective EDE Entity resubmits a complete audit, CMS will enter the resubmitted audit at the end of the review queue based on the date of submission. CMS does not guarantee any approval timelines.

Guidance and Program Materials (Updated)

CMS issued updated requirements, trainings (required for both Auditors and representatives of prospective EDE Entities), and baseline toolkits for the April 1, 2019 to June 30, 2019 submission window in early 2019. CMS primarily used the same content and requirements as

[2] Upstream EDE Entities must notify CMS of their participation by submitting an upstream documentation package (to be provided by CMS) at the time the primary EDE Entity submits its audits or after. There is no deadline to submit the upstream entity documentation package, but to be reasonably certain an upstream entity will be approved by November 1, 2019, CMS strongly recommends that Entities submit the required documentation no later than October 1, 2019 or as soon as feasible to allow time to review prior to activating their Partner IDs.

in the materials released in 2018 for PY 2019. Accordingly, prospective EDE Entities could begin developing their EDE environments based on the previous toolkits and privacy and security documentation that were located on CMS zONE.[3] Please note: the new baseline versions of the toolkits are also available on CMS zONE. Prospective EDE Entities should also refer to the Guidelines.[4]

CMS also provided further information about requirements for EDE Entities that were approved to use EDE for PY 2019 prior to the April 1, 2019 to June 30, 2019 submission window in the Guidelines.

2. What constitutes a complete Business Requirements Audit? (Updated)

CMS will review each audit submission for completeness. CMS will not accept incomplete audits.

A complete business requirements audit submission meets the following criteria, at a minimum:

Toolkit & Template	Minimum Requirements for a Complete Audit
All Toolkits	▪ Complete Auditor documentation (i.e., columns indicated for Auditor results) with no ambiguous language about the audit process or potential unmitigated risks ▪ All required rows of all toolkits are completed ▪ Risks identified during the course of the audit must be documented
Communications Toolkit	▪ Screenshots that demonstrate compliance (in English and Spanish, if applicable) when the applicable requirements require screenshots to be provided as evidence under the Requirements tab in the toolkit.
Application User Interface (UI) Toolkit	▪ Clear and adequate assessment of the Spanish-language application, if applicable ▪ *Note: The Application UI Toolkit must be reviewed in full. The Eligibility Results Test Cases do not cover all questions in the Application UI Toolkit*
Eligibility Results Toolkit(s)	▪ Screenshots of the entire application flow for each test case ▪ Correct eligibility results and eligibility determination notices (EDNs) for each test case
Application Program Interface (API) Functional Integration Toolkit	▪ Correct results and successful completion of each test case is documented
EDE Business Audit Report Template	▪ Complete descriptions of each requirement; Auditors must not exclude key aspects of each requirement
Supplemental Documentation Requested by CMS	▪ Submit all supplemental documentation and information requested by CMS ▪ CMS will not review supplemental documentation that CMS has not requested ▪ Auditors and prospective EDE Entities must not provide unrequested, supplemental documentation to communicate risks that are not otherwise appropriately documented in the Business Audit Report Template or Toolkits

[3] Note that prospective EDE Entities must set up a CMS Enterprise Portal account and request zONE access to view the zONE website. Prospective EDE Entities must share all EDE audit resources with their Auditors; CMS zONE site access is restricted to prospective and approved EDE Entities (participating web-brokers and issuers) only.

[4] *Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements* (February 19, 2019): https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Guidelines-for-Third-party-Auditors-EDE-PY19PY20.pdf

An incomplete business requirements audit does not meet the completeness criteria described above. The Auditor must complete incomplete audits in accordance with the standards described above. CMS will require that incomplete audits be resubmitted in their entirety and will prioritize its review of these resubmitted audits based on the date the complete audit is submitted.

Business requirements audits should not include comments that describe the Auditor’s process for verifying the requirement unless there is a specific issue or concern regarding the requirement that warrants raising a concern.

3. What constitutes a complete Privacy and Security Audit? (Updated)

CMS will review each audit submission for completeness. CMS will not accept incomplete audits.

A complete privacy and security audit submission meets the following criteria, at a minimum:

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 Assessment Report (SAR)	▪ The SAR is not a living document; findings should not be added/removed from the SAR unless CMS’ 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 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 Open Web Application Security Project (OWASP) Top 10. ▪ Only one 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.

Document	Minimum Requirements for a Complete Audit
Monthly Vulnerability Scans	▪ The EDE Entity must conduct monthly vulnerability scans for their 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 Strategy Guide (ISCM Guide)	▪ The ISCM Guide describes CMS's strategy for EDE Entities following the initial approval of the Request to Connect (RTC). This guide conveys the minimum requirements for EDE Entities that implement an ISCM program for their systems and to maintain ongoing CMS RTC approval. ▪ The ISCM describes the monthly, quarterly, and annual reporting summaries. ▪ The ISCM describes the security and privacy controls action frequencies. ▪ The ISCM describes the subset of security and privacy core controls that must be tested annually.

An incomplete privacy and security audit does not meet the completeness criteria described above. The Auditor must complete incomplete audits in accordance with the standards described above. CMS will require that incomplete audits be resubmitted in their entirety and will prioritize its review of these resubmitted audits based on the date the complete audit is submitted.

4. How can prospective EDE Entities implement EDE for calendar year 2019?

Prospective EDE Entities have two main options to consider in determining how and to what extent to pursue participation in EDE during calendar year 2019:

- Participate as a primary EDE Entity that has developed its own EDE environment and contracted with an Auditor to audit the environment,[5] or
- Participate as an upstream EDE Entity partner of an approved primary EDE Entity, which may not require an independent audit of the upstream entity's systems (i.e., primary EDE Entities may provide an EDE environment to another entity [e.g., an issuer or web-broker]).

All upstream EDE Entities must have a legal relationship with a primary EDE Entity. The list of EDE Entities (both primary and upstream) that are approved to use the EDE pathway is available here.[6] Prospective EDE Entities that are interested in learning more about upstream partnerships (either participating as a primary EDE Entity partnering with upstream EDE Entities or as an upstream EDE Entity) are encouraged to review the current Guidelines and forthcoming guidance.

[5] CMS is offering prospective EDE Entities three phases for hosting applications using the EDE pathway. A prospective EDE Entity may choose to implement Phase 1, 2, or 3 for the PY 2019 and PY 2020. For additional information on basic EDE program requirements and details, please refer to the *Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements* (February 19, 2019): https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Guidelines-for-Third-party-Auditors-EDE-PY19PY20.pdf

[6] This list is updated frequently, but it may not immediately reflect EDE Entities most recently approved to use the EDE pathway.