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: **February 19, 2019**
From: **Center for Consumer Information and Insurance Oversight**
Title: **Health Insurance Exchange Guidelines**
Subject: **Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements**

I. Summary

The Centers for Medicare & Medicaid Services (CMS) is continuing to implement Enhanced Direct Enrollment (EDE), an optional program allowing EDE Entities[1] (i.e., Qualified Health Plan [QHP] issuers and web-brokers seeking to participate in EDE[2]) registered with the Federally-facilitated Exchange (FFE or Exchange, also known as the Marketplace) and State-based Exchanges on the Federal Platform (SBE-FPs) to host an application for Marketplace coverage on their own websites. Participation in EDE requires integration with the Marketplace's standalone eligibility service (SES). The SES is a suite of application program interfaces (APIs) that will allow EDE Entities approved to participate in EDE to create, update, submit, and ultimately retrieve eligibility results for an application.

Based on the EDE implementation experience for the plan year (PY) 2019 open enrollment period (OEP), CMS is revising the program requirements for PYs 2019 (after the 2019 OEP) and 2020. This set of guidelines outlines EDE program and audit requirements for PY 2019 (after the OEP) and PY 2020. CMS will continue to support the classic DE pathway (also referred to as the "double redirect" pathway) for PY 2019 and PY 2020.

CMS offers audit submission windows when prospective EDE Entities may submit audits to apply for EDE participation. Audit submission windows are for prospective EDE Entities seeking to use the EDE pathway or for EDE Entities already approved to use the EDE pathway that are seeking to implement a new phase (see Section XI, Processes for Changes to an Audited or Approved EDE Environment, for more information on requirements for phase changes).

The primary audit submission window for prospective EDE Entities interested in implementing EDE in calendar year 2019 is from April 1, 2019 to June 30, 2019.[3] CMS will not review audits until the submission window begins. There is no guarantee that every prospective EDE Entity that submits a complete audit within the submission window will receive approval prior to the

[1] References to "EDE Entity" or "EDE Entities" throughout these guidelines encompass third-party administrators or other entities performing services on behalf of issuers or web-brokers.

[2] CMS uses the term "web-broker" to describe an individual agent or broker, group of agents and brokers, or company registered with the FFE that provides a non-Exchange website to assist consumers in the selection and enrollment in QHPs offered through the Exchanges as described in 45 C.F.R. § 155.220(c)(3).

[3] 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.

2020 OEP or during the 2019 calendar year. No prospective EDE Entity will be approved unless and until the Entity meets all program requirements. CMS will not review audits received after this submission window until the next submission window. CMS will release future guidance about the next annual audit submission window after the PY 2020 OEP.

II. Background

When using the EDE pathway, an EDE Entity will provide a full application,[4] enrollment, and post-enrollment support experience on its website, and must implement the full EDE API suite of required services. This suite of required services includes: Store ID Proofing, Person Search, Create App, Create App from Prior Year App, Store Permission, Get App, Add Member, Remove Member, Update App, Submit App, Get Data Matching Issue (DMI), Get Special Enrollment Period Verification Issue (SVI), Metadata Search, Notice Retrieval, Submit Enrollment, Document Upload, System and State Reference Data, and Get Enrollment. This list excludes optional APIs.

The EDE Entity will be able to transfer information directly between its application and the SES by integrating its unique user interface (UI) with the SES API suite. CMS will continue to be responsible for determining each consumer's eligibility and issuing Eligibility Determination Notices (EDNs).

CMS aims to foster a better consumer experience with the EDE pathway. EDE Entities and CMS will accomplish this objective by providing consumers in FFE and SBE-FP states with additional methods to shop and apply for Exchange coverage and by allowing consumers to work with an EDE Entity to enroll in a QHP without requiring consumers to log on to HealthCare.gov. Using the API suite, EDE Entities can innovate and implement improvements to the enrollment process. The EDE API suite will provide an EDE Entity with the data and tools necessary to fully manage customer relationships, including the ability to update applications when necessary, as well as to verify that consumers have effectuated policies, and assist consumers with remedying open consumer DMIs/SVIs and payment issues. CMS anticipates the EDE pathway will result in increased effectuation rates.

These guidelines define EDE program requirements and discuss requirements and considerations for prospective EDE Entities' selection of an Auditor, as well as the scope of the operational readiness review (ORR) prospective EDE Entities must undertake to demonstrate they are prepared to provide EDE services through use of the EDE pathway.

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. Each prospective EDE Entity must engage one or more independent Auditors to perform these audits and certify that the Entity's website(s) and operations comply with the program requirements listed in Exhibit 3 and Exhibit 5 of this guidance prior to CMS approving the Entity to use the EDE pathway.

[4] An EDE Entity's EDE environment and application may not support all applicant eligibility scenarios or application changes depending on the EDE Entity's chosen phase, as described below in Section IV.A, Application Phase Options.

The ORR process and CMS approval are necessary because of the effects an EDE Entity's processes may have on the HealthCare.gov information technology (IT) platform and consumers' eligibility applications.

CMS will conduct ongoing oversight of each EDE Entity in a manner consistent with that provided in previous plan years, including regular oversight of the Entity's applications in its production and testing environments for completeness and accuracy. Consistent with the application requirements detailed in this document and the EDE Business Agreement, CMS requires each prospective and approved EDE Entity using EDE to maintain a testing environment that accurately represents its EDE production environment and integration with the EDE pathway, including functional use of all EDE APIs.

A. Authority

Pursuant to 45 C.F.R. §§ 155.220(c)(3)(i), 155.221, 155.260, 156.265(b), and 156.1230, an EDE Entity must comply with applicable requirements, including demonstrating operational readiness to use the EDE pathway. The Department of Health & Human Services (HHS) may immediately suspend the EDE Entity's ability to transact information with the FFE if CMS discovers circumstances that pose unacceptable or unmitigated risk to FFE operations or FFE IT systems.

Pursuant to 45 C.F.R. § 155.221, a prospective EDE Entity must retain one or more independent third-party Auditors to validate compliance with program requirements (see Section V, Selection of an Auditor, for guidance pertaining to the selection of an Auditor). The prospective EDE Entity will identify the Auditor(s) it has selected for verifying program compliance in each of the two agreements the Entity must sign with CMS: an EDE Business Agreement, which sets forth consumer communication and operational requirements, and an Interconnection Security Agreement (ISA), which sets forth privacy and security requirements.

If a primary EDE Entity allows upstream EDE Entities to access its approved EDE environment, CMS will permit the Auditor(s) hired by the primary EDE Entity providing the EDE environment to conduct the audit of the environment for both the primary EDE Entity providing the environment and for the upstream EDE Entities accessing the environment.[5] Please note that EDE Entities accessing an approved EDE environment may not have to retain an Auditor or sign an ISA (see Section IV.B, Providing an EDE Environment to Other Entities, for more information about requirements for EDE Entities accessing an approved EDE environment).

CMS will consider Auditors to be downstream and delegated entities of a prospective EDE Entity in accordance with 45 C.F.R. § 156.340 and the QHP Issuer Agreement for QHP issuers, and in accordance with the Web-broker Agreement for web-brokers. The EDE Entity will be responsible for Auditor performance and for compliance with applicable program requirements.

[5] Please refer to Section IV, Enhanced Direct Enrollment Critical Decision Factors, for more information about primary EDE Entities and upstream EDE Entities.

III. Information for Existing EDE Entities

A. EDE Entities That CMS Approved to Use the EDE Pathway

For existing EDE Entities that were approved to use the EDE pathway for PY 2019 and are not changing their EDE phase for PY 2020, CMS aims to mitigate the burden of the audit renewal process for the PY 2020 OEP.

i. Business Requirements Audit

Existing EDE Entities pursuing a different EDE phase from the phase CMS initially approved should refer to Section XI.A, EDE Entity-initiated EDE Phase Change Requests, for the requirements and process to implement an EDE Entity-initiated phase change request (CR). Existing EDE Entities that are not pursuing a different EDE phase do not need to submit a new business requirements audit. Accordingly, existing EDE Entities that are not pursuing a different phase do not need to contract with a business requirements Auditor, but they may need to implement CMS-initiated CRs as described in Section XI.B, CMS-initiated Change Requests, of these Guidelines.

ii. Privacy and Security Audit

EDE Entities must adhere to the continuous monitoring reporting requirements in the *Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide* (ISCM Strategy Guide), which includes the completion of an annual assessment of security and privacy controls described in the ISCM.

B. EDE Entities That Have Completed Their Audits, But That CMS Has Not Approved

i. *Business Requirements Audit*

For a prospective EDE Entity that is not approved for PY 2019, but has submitted a complete business requirements audit prior to the release of these guidelines, CMS will allow such a prospective EDE Entity to use its previously submitted and complete EDE Business Audit and it will not be required to submit a new audit assuming it continues to seek approval for the phase indicated in its initial audit submission. The prospective EDE Entity must implement any changes to the business requirements as detailed in the CMS-initiated CR process.

ii. Privacy and Security Audit

For a prospective EDE Entity that is not approved for PY 2019, but has submitted a complete privacy and security audit prior to the release of these guidelines and no significant changes have been made to its environment since the submission, pursuant to the processes defined below in Section XI, Processes for Changes to an Audited or Approved EDE Environment, CMS will allow such a prospective EDE Entity to use its previously submitted and complete EDE privacy and security audit and it will not be required to submit a new audit. Consistent with the ISCM Strategy Guide, prospective EDE Entities may need to provide updated privacy and security documentation to CMS to demonstrate the continued compliance of the environment. CMS will only allow this approach to the extent that the previous audit accurately represents a prospective EDE Entity’s current compliance standing.

IV. Enhanced Direct Enrollment Critical Decision Factors

Prospective EDE Entities have several options to consider in determining how and to what extent to participate in EDE during calendar year 2019. An Entity may participate as a *primary EDE Entity* that has developed its own EDE environment or may participate as an *upstream EDE Entity* partner of an approved primary EDE Entity. Please see Section IV.B, Providing an EDE Environment to Other Entities, for more information.

A. Application Phase Options

CMS is offering prospective EDE Entities the option of implementing one of three phases of the eligibility application using the EDE pathway. A prospective EDE Entity may choose to implement Phase 1, 2, or 3 for PY 2019 and for the PY 2020 OEP (described further below). A prospective EDE Entity must commit to a phase and complete the phase implementation prior to initiating its audit because the audit must reflect the compliance of the prospective EDE Entity's operational EDE environment with the requirements of the applicable phase. After conducting and submitting an audit, prospective and approved EDE Entities must not modify their EDE environments to change phases without consulting CMS and pursuant to the processes defined below in Section XI, Processes for Changes to an Audited or Approved EDE Environment.

EDE Entities that implement Phases 1 or 2 are required to implement screening questions to redirect consumers whose circumstances the EDE Entities are unable to support to other supported application and enrollment channels. EDE Entities, of any phase, will be required to support consumer-reported changes in circumstances (CiCs) and special enrollment periods (SEPs) during and outside of the OEP, as well as supporting re-enrollment application activities. Exhibit 1 describes each of the three end-state phases and explains their benefits.

Exhibit 1. Application End-state Phases

End State Phases	Description	Benefits
Phase 1: Host Simplified Application + EDE API Suite	EDE Entity hosts an application that cannot support all application scenarios but will support only a subset of application scenarios. ▪ Application filer (and others on application, if applicable) resides in the application state and all dependents have the same permanent address, if applicable ▪ Application filer plans to file a federal income tax return for the coverage year; if married plans to file a joint federal income tax return with spouse ▪ Application filer (and spouse, if applicable) is not responsible for a child 18 or younger who lives with the Application filer but is not on his/her tax return ▪ No household members are full-time students aged 18-22 ▪ No household member is pregnant or has had a child in the last 60 days ▪ All applicants are U.S. citizens ▪ All applicants can enter Social Security Numbers (SSNs) ▪ No applicants are applying under a name different than the one on his/her Social Security cards ▪ No applicants were born outside of the U.S. and became naturalized or derived U.S. citizens ▪ No applicants are currently incarcerated (detained or jailed) ▪ No applicants are American Indian or Alaska Native ▪ No applicants are offered health coverage through a job or COBRA ▪ No applicants were in foster care at 18 and are currently 25 or younger ▪ All dependents are claimed on the Application filer's federal income tax return for the coverage year ▪ All dependents are the Application filer's children who are single (not married) and 25 or younger ▪ No dependents are stepchildren or grandchildren ▪ No dependents live with a parent who is not on the Application filer's tax return	Lowest level of effort to implement and audit. EDE development would be streamlined, since not all application questions would be in scope.
Phase 2: Host Expanded Simplified Application + EDE API Suite	EDE Entity hosts an application that cannot support all application scenarios. The scenarios supported include the following: ▪ All scenarios covered by Phase 1 ▪ Full-time student ▪ Pregnant application members ▪ Non-U.S. citizens ▪ Naturalized U.S. citizens ▪ Application members who do not provide an SSN ▪ Application members with a different name than the one on their SSN cards ▪ Incarcerated application members ▪ Application members who previously were in foster care ▪ Stepchildren	Second lowest level of effort to implement and audit. EDE development would be streamlined, since not all application questions would be in scope.

End State Phases	Description	Benefits
Phase 3: Host Complete Application + EDE API Suite	EDE Entity hosts an application that supports all application scenarios (equivalent to existing HealthCare.gov): ▪ All scenarios covered in Phase 2 ▪ American Indian and Alaskan Native application members ▪ Application members with differing home addresses or residing in a state separate from where they are applying for coverage ▪ Application members with no home address ▪ Application members not planning to file a tax return ▪ Married application members not filing jointly ▪ Application members responsible for a child 18 or younger who lives with them, but is not included on federal tax return (parent/caretaker relative questions) ▪ Application members offered coverage through their job, someone else's job, or COBRA ▪ Application members with dependent children who are over 25 or who are married ▪ Application members with dependent children (under 21) who are not applying for coverage ▪ Application members with dependent children living with a parent not on their federal tax return ▪ Dependents who are not sons/daughters	Highest level of effort to implement and audit. EDE Entity would provide and service the full range of consumer scenarios. Additionally, the EDE Entity would no longer need to redirect consumers to alternative pathways for complex eligibility scenarios. Please note that the implementation of Phase 3 is comparatively more complex than the other phases and may require more time to audit and approve.

In addition to the Application UI, EDE Entities are required to provide account management functions for consumers and conduct communications about their application and enrollment status. These communications include, but are not limited to, providing status updates on the application and enrollment, DMIs and SVIs, enrollment periods, notices that are generated by the FFE, facilitating document uploads for DMIs and SVIs, and updating and reporting changes to application and enrollment information. To review more detailed descriptions of communications requirements, please refer to the most recent version of the Communications Toolkit, which is available on CMS zONE.[6]

B. Providing an EDE Environment to Other Entities

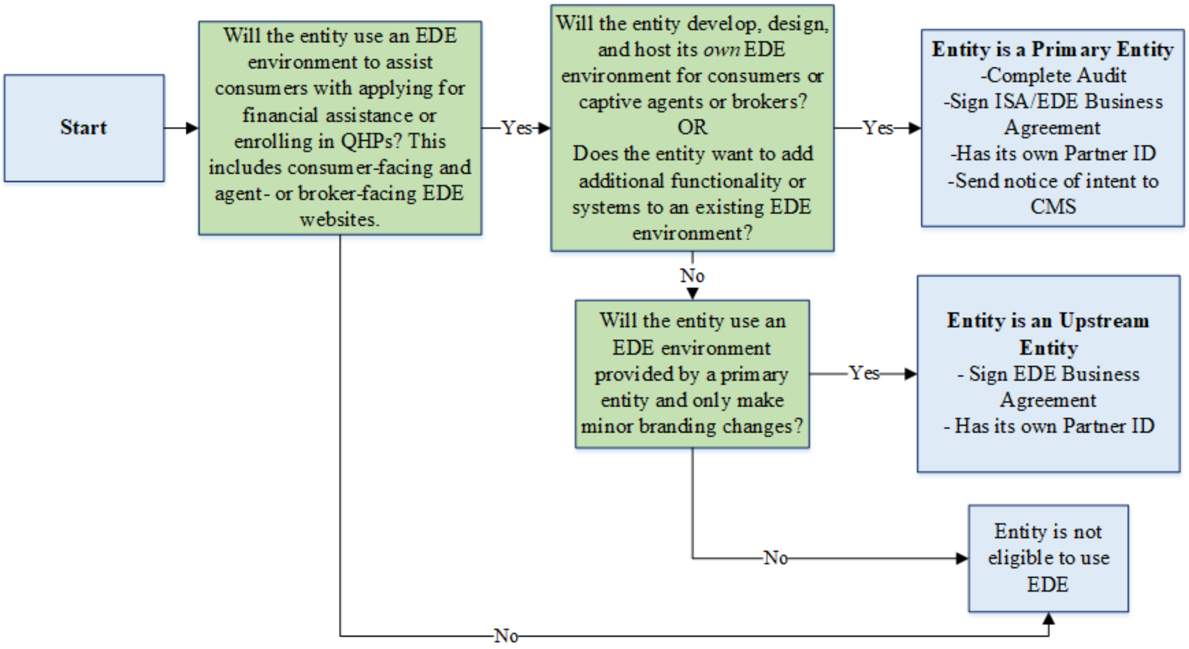
EDE Entities that provide an EDE environment to another entity (e.g., an issuer or web-broker) are referred to as primary EDE Entities. The Entity that is provided the environment by the primary EDE Entity is referred to as an upstream EDE Entity.[7] To determine whether an entity is an upstream EDE Entity or a primary EDE Entity, CMS has provided the chart shown as Exhibit 2, which details the responsibilities and obligations that determine whether an entity would be considered an upstream EDE Entity for purposes of this section. All upstream EDE Entities must have a legal relationship with a primary EDE Entity reflected in a signed written agreement between the upstream EDE Entity and the primary EDE Entity.

[6] EDE documents and materials will be posted at the following link on CMS zONE: https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials.

[7] The list of EDE Entities (both primary and upstream) that are approved so far to use EDE for plan year 2019 is available here: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Web-brokers-in-the-Health-Insurance-Marketplace.html (see "Enhanced Direct Enrollment Approved Partners").

A primary EDE Entity is an entity that will either 1) develop, design, and host its own EDE environment for consumers or captive agents or brokers or 2) add additional functionality or systems to an existing EDE environment. A primary entity must complete an audit, sign the ISA and EDE Business Agreement, have its own Partner ID, and send a notice of intent to CMS. An upstream EDE Entity is an entity that will use an EDE environment provided by a primary EDE Entity and will only make minor branding changes to an EDE environment. An upstream EDE Entity must sign the EDE Business Agreement and have its own Partner ID.

Exhibit 2: Primary vs. Upstream Decision Flow


Start
Will the entity use an EDE environment to assist consumers with applying for financial assistance or enrolling in QHPs? This includes consumer-facing and agent- or broker-facing EDE websites.
Yes
Will the entity develop, design, and host its *own* EDE environment for consumers or captive agents or brokers?
OR
Does the entity want to add additional functionality or systems to an existing EDE environment?
Yes
Entity is a Primary Entity
-Complete Audit
-Sign ISA/EDE Business Agreement
-Has its own Partner ID
-Send notice of intent to CMS
No
Will the entity use an EDE environment provided by a primary entity and only make minor branding changes?
Yes
Entity is an Upstream Entity
- Sign EDE Business Agreement
- Has its own Partner ID
No
Entity is not eligible to use EDE
No

i. Standards Regarding Primary EDE Entities and Upstream EDE Entities

CMS will permit an Entity to develop and provide its approved EDE environment to one or more upstream EDE Entities. The primary EDE Entity—the Entity providing the EDE environment to other Entities—is responsible for contracting with one or more independent Auditors to perform the business requirements audit and the privacy and security audit. Upstream EDE Entities do not have to perform independent audits to the extent they are using their primary EDE Entity's EDE environment with no modifications other than modifications to display different branding.

The primary EDE Entity developing the EDE environment and any upstream EDE Entity using that environment (e.g., QHP issuers) must both submit an EDE Business Agreement and confirm the existence of a signed, written agreement between the two Entities in writing to CMS. The upstream EDE Entity will be responsible for complying with all requirements in regulation; applicable guidance; and the EDE Business Agreement, including oversight of the primary EDE Entity providing the EDE environment.

- If an upstream EDE Entity will use a primary EDE Entity's approved EDE environment, but the upstream EDE Entity adds additional functionality or systems to complete the implementation of its own EDE environment (e.g., the approved EDE environment of the primary EDE Entity does not comprise the entire EDE environment for an upstream EDE

Entity), the upstream EDE Entity will need to contract with an independent Auditor to conduct and submit supplementary business and privacy and security audits with any additional findings for the added functionality or systems to confirm the upstream EDE Entity's compliance with applicable CMS regulations and the EDE Business Agreement, as appropriate.

- If an upstream EDE Entity is using an approved EDE environment and the associated audit packages provided by a primary EDE Entity, the upstream EDE Entity must indicate in its EDE Business Agreement that it is using an approved EDE environment provided by a primary EDE Entity and be prepared to submit a copy of that primary EDE Entity's business requirements audit package, privacy and security audit package, and documentation of the arrangement upon request by CMS.
- If an upstream EDE Entity will use an approved EDE environment provided by a primary EDE Entity, but the primary EDE Entity's environment will not comprise the totality of the upstream EDE Entity's implementation of its own EDE environment (consistent with the example above), the upstream EDE Entity must submit two audit packages that contain both the results of the audits for the EDE environment provided by the primary EDE Entity, as well as the results of the audits that cover any additional systems or requirements that complete the upstream EDE Entity's EDE environment.

CMS will require written confirmation from both primary EDE Entities and their upstream Entities about any such relationships, as well as require information and documentation from the upstream EDE Entities as requested. CMS requires written confirmation from both the primary EDE Entity and upstream EDE Entity to allow a connection to CMS for an upstream EDE Entity. Additionally, primary EDE Entities must identify inheritable common and hybrid security and privacy controls that their upstream EDE Entities should leverage. The common and hybrid security and privacy controls must be documented in the EDE System Security and Privacy Plan (SSP) workbook, and must also be documented as part of the written contract between primary EDE Entities and their upstream EDE Entities.

ii. Unique Partner ID Requirements for Primary EDE Entities and Upstream Entities

CMS will be requiring primary EDE Entities with upstream EDE Entities to submit EDE API transactions using Partner IDs associated with the upstream EDE Entities, when EDE applications/enrollments originate from the upstream EDE Entities. CMS will not require a Partner ID for an agent or broker that uses a primary EDE Entity's platform by redirecting consumers to the primary EDE Entity's site/URL to complete an application and enrollment.

CMS is requiring this:

- For reporting and tracking purposes, the application/enrollment must reflect the EDE Entity that the transaction originated from.
- For purposes of suspension, if applicable, CMS will be able to suspend specific Partner IDs. If only one Partner ID is used by the primary EDE Entity, a suspension of either the primary EDE Entity or any single upstream EDE Entity would result in the suspension of all activity from any EDE Entity using that Partner ID.

A primary EDE Entity that has upstream EDE Entities must update its Hub[8] Onboarding Form, to include additional information for each of its upstream EDE Entities. The Hub Onboarding Form can be found on CMS zONE,[9] and when completed, must be emailed to the email address included on zONE and in the Hub Onboarding Form (dsh.support@qssinc.com as of February 2019). Each upstream EDE Entity must have a unique Partner ID and will receive its Partner ID when its primary EDE Entity updates its Hub Onboarding Form. In addition, prior to submitting its business requirements audit, a prospective primary EDE Entity that intends to allow upstream EDE Entities to use its EDE environment must notify CCIIO of the name, Partner ID, and primary point of contact (POC) of each prospective upstream EDE Entity that will use its EDE environment with its business audit submission. Alternatively, if the primary EDE Entity is adding upstream EDE Entities after its audit submission and/or approval to participate in EDE, then the primary EDE Entity must submit this information by contacting the DE Help Desk at directenrollment@cms.hhs.gov in addition to updating its Hub Onboarding form.

C. Data Collections

An EDE Entity must perform data collections only within its approved EDE environment, and cannot collect consumer information for purposes of the EDE pathway on any website other than websites identified in the EDE Entity's audit submitted to CMS. Any and all websites that collectively make up an EDE Entity's EDE environment will be subject to oversight by CMS. Any implementation of an EDE Entity's EDE environment must be consistent with the audit submitted to and approved by CMS.

D. Downstream Third-party Agent and Broker Arrangements

An EDE Entity may allow individual third-party agents and brokers who are validly registered with the FFE to use its respective approved EDE environment to assist consumers in supported states (i.e., states in which the EDE Entity operates) with applying for coverage, as well as advanced payments of the premium tax credit (APTC) and Cost-Sharing reductions (CSRs), and with selecting QHPs. However, the EDE Entity must not provide the capability for individual third-party agents or brokers or other downstream and delegated entities[10] or individuals who are not or will not be a party to their own EDE Business Agreement with CMS to use its EDE environment on the third-party's own website or otherwise outside of the EDE Entity's approved website and EDE environment.

Additionally, an EDE Entity is responsible for ensuring compliance with the terms and conditions of the EDE Business Agreement by all individual downstream third-party agents and brokers who access and use its approved EDE environment. An EDE Entity's environment must contain sufficient privacy and security safeguards and must be accessed consistent with its documented policies and procedures, to protect against noncompliance with respect to the EDE Business Agreement by any authorized individual downstream agents and brokers who are using the EDE environment or interacting with or managing any consumer applications associated with the EDE environment. For example, while CMS does not require individual downstream agents

[8] EDE Entities must connect to the Data Services Hub ("Hub") in order to access and use the FFE APIs.

[9] The Hub Onboarding Form is available at the following CMS zONE webpage: https://zone.cms.gov/document/hub-onboarding-form.

[10] Downstream and delegated entities are defined in accordance with 45 C.F.R. § 156.340 and the QHP Issuer Agreement for QHP issuers, and in accordance with the Web-broker Agreement for web-brokers.

or brokers who will use an EDE Entity's EDE environment to sign the EDE ISA independently, CMS does require that the written agreement between the EDE Entity and the agent or broker require the agent or broker to comply with the relevant and applicable privacy and security requirements contained within the Agent and Broker Agreement "Appendix A: Privacy and Security Standards and Implementation Specifications for Non-Exchange Entities to the Agreement between Agent or Broker and the Centers for Medicare & Medicaid Services for Individual Market Federally-Facilitated Exchanges and the State-Based Exchanges on the Federal Platform." Furthermore, a compliant EDE environment that is appropriately managed by an EDE Entity must protect against noncompliant use of the environment by individual downstream agents or brokers with respect to EDE privacy and security standards.

V. Selection of an Auditor

A prospective EDE Entity must enter into a written agreement with each independent Auditor it selects. Pursuant to its downstream and delegated entity oversight authority, CMS may request a copy of all documentation related to a prospective EDE Entity's engagement of its Auditor(s) and the Auditor(s)' work in relation to the engagement. Each prospective EDE Entity must identify its selected Auditor(s) in the EDE Business Agreement and the ISA between CMS and the EDE Entity.

A. Allowance for Multiple Auditors

A prospective EDE Entity is permitted to select either one Auditor to complete both the business requirements audit and the privacy and security audit or the prospective EDE Entity may select two Auditors, one to complete the business requirements audit and the other to complete the privacy and security audit. If the prospective EDE Entity selects only one Auditor, that Auditor may choose to conduct either the business requirements audit or the privacy and security audit only, and subcontract with another Auditor to conduct the other audit.

When a prospective EDE Entity retains two Auditors to complete the audits, it should notify CMS of this arrangement and provide the contact information for both Auditors, including for the subcontractor of an Auditor, if applicable. In such cases, both the Auditor and subcontractor of the Auditor will be considered downstream or delegated entities of the prospective EDE Entity. Auditors are permitted to subcontract these activities; however, a prospective EDE Entity must disclose any subcontracting arrangements by its Auditors in the EDE Business Agreement and/or ISA with CMS and disclose any potential conflicts of interest consistent with the EDE Business Agreement.

B. Business Requirements Auditor Experience

HHS will require that a prospective EDE Entity selects Auditor(s) with the experience outlined below and attest, within the EDE Business Agreement and the ISA, that the Auditor(s) have demonstrated or possess such experience.

i. Required Business Requirements Auditor Experience

CMS will require that the Auditor selected by prospective EDE Entities to conduct the business requirements audit possess audit experience, which an Auditor may demonstrate through experience conducting operational audits or similar services for federal, state, or private programs. A prospective EDE Entity may consider an Auditor to be qualified to conduct the business requirements audit if key Auditor personnel possess one or more of the following relevant auditing certifications: Certified Internal Auditor (CIA), Certification in Risk Management Assurance (CRMA), Certified Information Systems Auditor (CISA), or Certified Government Auditing Professional (CGAP).

ii. Recommended Business Requirements Auditor Experience

CMS recommends that an Auditor conducting the business requirements audit has minimum technical experience with XML and JavaScript Object Notation (JSON). Most of the new EDE APIs will be in JSON format; however, some will be in XML format. A general familiarity and understanding of XML and JSON request and response structure may be useful to an Auditor conducting the business requirements audit. The necessity of this experience may depend on the Auditor's approach to reviewing the prospective EDE Entity's environment and if the prospective EDE Entity provides information relevant to the audit in a user-friendly interface or in raw XML or JSON file format. CMS anticipates providing limited training and technical assistance to prospective EDE Entities and Auditors on understanding and reading the EDE XML and JSON files.

C. Privacy and Security Auditor Experience

i. Required Privacy and Security Auditor Experience

CMS will require that the key personnel of an Auditor selected by a prospective EDE Entity to conduct the privacy and security audit possess a combination of privacy and security experience and relevant auditing certifications. Examples of acceptable privacy and security experience include: 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 National Institute of Standards and Technology (NIST) SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*; and reviewing compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule standards. Examples of relevant auditing certifications are: 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).

In determining whether an Auditor has an acceptable combination of privacy and security experience and relevant auditing certifications, a prospective EDE Entity may substitute extensive FISMA experience for multiple privacy and security certifications.

The Auditor must be familiar with NIST standards, HIPAA, and other applicable federal privacy and cybersecurity regulations and guidance. In addition, the Auditor must be capable of performing penetration testing and vulnerability scans on all interfaces that collect personally identifiable information (PII) or connect to CMS.

ii. Recommended Privacy and Security Auditor Experience

CMS strongly recommends that an Auditor selected to conduct the privacy and security audit have prior FISMA experience and/or is listed on the FedRAMP-certified third-party assessment organization website.[11] Prior FISMA experience is recommended in order for an Auditor to appropriately assess a prospective EDE Entity's compliance with the required privacy and security controls and produce a high-quality comprehensive Security and Privacy Controls Assessment Test Plan (SAP) and Security and Privacy Assessment Report (SAR).

D. Conflict of Interest and Auditor Independence and Objectivity

i. Conflict of Interest

A prospective EDE Entity must select an Auditor who is free from any real or perceived conflicts of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence. A prospective EDE Entity must disclose to HHS any financial relationship between the Auditor and individuals who own or are employed by the Auditor or who own or are employed by an agent, broker, or QHP issuer for which the Auditor is conducting an ORR pursuant to 45 C.F.R. §§ 155.220(c)(3)(i)(K) or 156.1230(b)(2) or a privacy and security audit pursuant to 45 C.F.R. §§ 155.280.

ii. Auditor Independence and Objectivity

A prospective EDE Entity's Auditor must remain independent and objective throughout the audit process for both audits. An Auditor is independent if there is no perceived or actual conflict of interest involving the developmental, operational, and/or management chain associated with the system and the determination of security and privacy control effectiveness or business requirement compliance. The Auditor's role is to provide an independent assessment of the compliance of the prospective EDE Entity's EDE environment and to maintain the integrity of the audit process. Upon submission of the audit, Auditors will be required to attest to their independence and objectivity in completing the audit, and that neither the prospective EDE Entity nor the Auditor took any actions that might impair the objectivity of the findings in the audit.

VI. Business Audit Requirements and Scope

An Auditor will complete a business requirements audit to ensure the prospective EDE Entity has complied with applicable requirements as defined in this guidance. A prospective EDE Entity must submit the resulting business requirements audit package to CMS. The Auditor may define its own methodology to conduct the business requirements audit within the parameters defined in Exhibit 3, which summarizes the review areas and review standards for the business requirements.

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

Exhibit 3. Business Requirements

Review Category	Requirement and Audit Standard
Identity Proofing Implementation	▪ *Requirement*: The EDE Entity must conduct identity proofing for Consumers entering the EDE Pathway for enrollments through both Consumer and in-person Agent/Broker pathways. EDE Entity must conduct identity proofing prior to submitting a Consumer's application to the FFE. If EDE Entity is unable to complete identity proofing of the Consumer, EDE Entity may either direct the Consumer to traditional double-redirect pathway or direct Consumer to the FFE (HealthCare.gov or the Marketplace Call Center at 1-800-318-2596 [TTY: 1-855-889-4325]. – Remote Identity Proofing/Fraud Solutions Archive Reporting Service (RIDP/FARS) or Third-Party Identity Proofing Services: CMS will make the FFE RIDP/FARS or other third-party identity proofing service available. EDE Entity does not need to use third-party identity proofing if it already uses the approved FFE RIDP service. If EDE Entity uses the FFE RIDP service, it must use the RIDP service only after confirming the Consumer is seeking coverage in a state supported by the FFE/federal platform, but prior to submitting the application. If EDE Entity uses a third-party identity proofing service, the service must be Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions (TFS)-approved, and EDE Entity must be able to produce documentary evidence that each Applicant has been successfully identity proofed. Documentation related to a third-party service could be requested in an audit or investigation by CMS (or its designee), pursuant to the EDE Business Agreement. Applicants do not need to be ID proofed on subsequent interactions with EDE Entity if the Applicant creates an account (i.e., username and password) on EDE Entity's website. ▪ Review Standard: – If EDE Entity uses the FFE RIDP service, the Auditor must verify that the EDE Entity has successfully passed testing with the Hub. – If EDE Entity uses a third-party identity proofing service, the Auditor must evaluate and certify the following: o The identity proofing service is FICAM TFS-approved, and o The EDE Entity has implemented the service correctly.
Phase-dependent Screener Questions (EDE Phase 1 and 2 EDE Entities Only)	▪ *Requirement:* An EDE Entity that implements either EDE Phase 1 or Phase 2 must implement screening questions to identify Consumers whose eligibility circumstances EDE Entity is unable to support consistent with the eligibility scenarios supported by EDE Entity's selected EDE phase. These phase-dependent screener questions must be located at the beginning of the EDE application, but may follow the QHP plan compare experience. For those Consumers who won't be able to apply through the EDE phase EDE Entity implements, EDE Entity must either route the Consumer to the traditional DE double-redirect pathway or direct the Consumer to the FFE (HealthCare.gov or the FFE Call Center at 1-800-318-2596 [TTY: 1-855-889-4325]). ▪ *Review Standard*: The Auditor must verify the following: – The EDE Entity has implemented screening questions—consistent with the requirements in the FFE Application UI Principles document and Application UI Toolkit—to identify Consumers with eligibility scenarios not supported by EDE Entity's EDE environment. – The EDE Entity's EDE environment facilitates moving Consumers to one of the alternative enrollment pathways described immediately above.

Review Category	Requirement and Audit Standard
Accurate and Streamlined Eligibility Application User Interface (UI)	▪ *Requirement*: EDE Entities using the EDE Pathway must support all application scenarios outlined in EDE Entity's selected phase. EDE Entity must adhere to the guidelines set forth in the FFE Application UI Principles document when implementing the application. EDE Entities can access the FFE Application UI Principles document on the CMS zONE EDE Documents and Materials webpage (https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials). Auditors will need to access the FFE Application UI Principles document to conduct the audit. – As explained in the FFE Application UI Principles document, EDE Entity must implement the application in accordance with the FFE requirements. For each applicable eligibility scenario, EDE Entity must display all appropriate eligibility questions and answers, including all questions designated as optional. (Note: These questions are optional for the Consumer to answer, but are not optional for EDE Entities to implement.) The FFE Application UI Principles document and Application UI Toolkit define appropriate flexibility EDE Entities may implement with respect to question wording, question order or structure, format of answer choices (e.g., drop-down lists, radio buttons), and integrated help information (e.g., tool tips, URLs, help boxes). In most cases, answer choices, question logic (e.g., connections between related questions), and disclaimers (e.g., advanced payments of the premium tax credit [APTC] attestation) must be identical to those of the FFE. – EDE Entities will also need to plan their application's back-end data structure to ensure that attestations can be successfully submitted to Standalone Eligibility Service (SES) application programming interfaces (APIs) at appropriate intervals within the application process and that EDE Entity can process responses from SES and integrate them into the UI question flow logic, which is dynamic for an individual Consumer based on his or her responses. EDE Entity will need to ensure that sufficient, non-contradictory information is collected and stored such that accurate eligibility results will be reached without any validation errors. ▪ *Review Standard*: The Auditor must review and certify the following: – The FFE Application UI has been implemented in EDE Entity's environment in accordance with the FFE Application UI Principles document. – The FFE Application UI displays all appropriate eligibility questions and answers from the Application UI Toolkit, including any questions designated as optional. – The Auditor will review the application for each supported eligibility scenario under the phase the EDE Entity has implemented to confirm that the application has been implemented in accordance with the FFE Application UI Principles document and Application UI Toolkit. The Auditor will document this compliance in the Application UI Toolkit. o Note: The phrase "supported eligibility scenario" does not refer to the Eligibility Results Toolkit scenarios. Auditors must verify that EDE Entities can support all scenarios supported by the EDE Entity's selected phase and this scope exceeds the scope of the test cases in the Eligibility Results Toolkits. – If EDE Entity has implemented Phase 1 or Phase 2, the Auditor will confirm that the UI includes a disclaimer stating that the environment does not support all use cases and application scenarios, and identifying which scenarios are and are not supported. The disclaimer should direct the Consumer to alternative pathways, such as the traditional DE double-redirect pathway or direct the Consumer to the FFE (HealthCare.gov or the FFE Call Center at 1-800-318-2596 (TTY: 1-855-889-4325). This requirement is included in the Communications Toolkit.

Review Category	Requirement and Audit Standard
Post-eligibility Application Communications	▪ *Requirement*: The application must display high-level eligibility results, next steps for enrollment, and information about each Applicant's program eligibility, Data Matching Issues (DMIs), special enrollment periods (SEPs), SEP Verification Issues (SVIs), and enrollment steps in a clear, comprehensive and Consumer-friendly way. – EDE Entity must provide Consumers with the CMS-provided Eligibility Determination Notices (EDNs) generated by the FFE any time it submits or updates an application pursuant to requirements provided by CMS in the Communications Toolkit. – EDE Entity must provide the EDN in a downloadable format at the time the Consumer's application is submitted or updated and must have a process for providing access to the Consumer's most recent EDN via the API. The UI requirements related to accessibility of a Consumer's EDN are set forth in the Communications Toolkit. – EDE Entity must provide and communicate status updates and access to information for Consumers to manage their application and coverage. These communications include, but are not limited to, status of DMIs and SVIs, enrollment periods, providing and communicating about new notices generated by the FFE, application and enrollment status, and supporting document upload for DMIs and SVIs. This requirement is detailed in the Communications Toolkit. ▪ *Review Standard*: The Auditor must verify and certify the following: – The EDE Entity's EDE environment is compliant with the requirements in the Communications Toolkit. – The EDE Entity's EDE environment notifies Consumers of their eligibility results prior to QHP submission, including when submitting a change in circumstances (CiC) in the environment. For example, if a Consumer's APTC or CSR eligibility changes, EDE Entity must notify the Consumer of the change and allow the Consumer to modify his or her QHP selection (if SEP-eligible) or APTC allocation accordingly. – EDE Entity must have a process for providing Consumers with a downloadable EDN in its EDE environment and for providing access to a current EDN via the API. EDE Entity must share required eligibility information that is specified by CMS in the Communications Toolkit. – The Auditor must verify that EDE Entity's EDE environment is providing status updates and ongoing communications to Consumers according to CMS requirements in the Communications Toolkit as it relates to the status of their application, eligibility, enrollment, notices, and action items the Consumer needs to take.
Accurate Information about the Exchange and Consumer Communications	▪ *Requirement:* EDE Entity must provide Consumers with CMS-provided language informing and educating the Consumers about the Exchanges and HealthCare.gov and Marketplace-branded communications Consumers may receive with important action items. CMS defines these requirements in the Communications Toolkit. ▪ *Review Standard:* The Auditor must verify and certify that the EDE Entity's EDE environment includes all required language, content, and disclaimers provided by CMS in accordance with the requirements stated in guidance and the Communications Toolkit.
Documentation of Interactions with Consumer Applications or the Exchange	▪ *Requirement:* EDE Entity must implement tracking metrics on its EDE environment to track Agent, Broker, and Consumer interactions, as applicable, with Consumer applications using a unique identifier for each individual, as well as an individual's interactions with the Exchanges (e.g., application; enrollment; handling of action items, such as uploading documents to resolve a DMI). ▪ *Review Standard:* The Auditor must verify EDE Entity's process for determining and tracking when an Agent, Broker, and Consumer has interacted with a Consumer application or taken actions utilizing the EDE environment. The Auditor must verify and certify the following: – The EDE Entity's environment tracks, at a minimum, the interactions of Agents, Brokers, and Consumers with a Consumer's account, records, application, or enrollment information. – The EDE Entity's environment tracks when an Agent, Broker, or Consumer views a Consumer's record, enrollment information, or application information. – The EDE Entity's environment uses unique identifiers to track and document activities by Consumers, Agents, and Brokers using the EDE environment. – The EDE Entity's environment stores this logged information for 10 years.

Review Category	Requirement and Audit Standard
Eligibility Results Testing and SES Testing	▪ *Requirement*: EDE Entity must submit accurate applications through the EDE Pathway that result in accurate and consistent eligibility determinations for the Consumer eligibility scenarios covered by EDE Entity's chosen EDE phase. – The business requirements audit package must include testing results in the designated FFE EDE testing environment. CMS has provided a set of Eligibility Results Toolkits with the eligibility testing scenarios on CMS zONE EDE Documents and Materials webpage (https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials). ▪ *Review Standard*: The Auditor must verify and certify the following: – The Auditor was able to successfully complete a series of test eligibility scenarios using EDE Entity's EDE environment implementation using the Eligibility Results Toolkits. For example, these scenarios may include Medicaid and Children's Health Insurance Program (CHIP) eligibility determinations, and different combinations of APTC and CSRs. Note: These scenarios do not test, and are not expected to test, every possible question in the Application UI flow for an EDE Entity's selected phase. In addition to reviewing the eligibility results test cases, the Auditor must review the Application UI for compliance as defined above. – The Auditor must test each scenario and verify that the eligibility results and the eligibility process were identical to the expected results and process. CMS will require the Auditor to provide confirmation that each relevant eligibility testing scenario was successful, that the expected results were received (as defined in the Eligibility Results Toolkits), and to submit screenshots, EDNs, and FFE Application IDs, when applicable, for each test scenario.
API Functional Integration Requirements	▪ *Requirement*: EDE Entity must implement the EDE API suite in accordance with the API specifications provided by CMS. The EDE API specifications are available on CMS zONE EDE Documents and Materials webpage (https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials). ▪ *Review Standard:* The Auditor must complete a set of Consumer testing scenarios to confirm that EDE Entity's API integration performs the appropriate functions when completing the application; these scenarios are available in the API Functional Integration Toolkit. For example, the Auditor may have to complete a scenario to verify that a Consumer is able to add individuals to the application and, if eligible, to the Consumer's coverage through the CiC process and that the API provides the expected response from the FFE. Some of the test cases require that the Auditor and EDE Entity request CMS to process application actions; the Auditor cannot mark these particular test cases as compliant until evaluating whether the expected outcome occurred after CMS takes the requested action.
Application UI Validation	▪ *Requirement:* EDE Entity must implement CMS-defined validation requirements within the application. The validation requirements prevent EDE Entity from submitting incorrect data to the FFE. ▪ *Review Standard:* The Auditor must confirm that EDE Entity's application has implemented the appropriate field-level validation requirements consistent with CMS requirements. These field-level validation requirements are documented in the FFE Application UI Principles document.

Review Category	Requirement and Audit Standard
Section 508-compliant UI	▪ *Requirement:* Pursuant to 45 C.F.R. § 155.220(c)(3)(ii)(D) (citing 45 C.F.R. §§ 155.230 and 155.260) and 45 C.F.R. § 156.265(b)(3)(iii) (citing 45 C.F.R. §§ 155.230 and 155.260), web-brokers and QHP issuers participating in DE, including all EDE Entities must implement an eligibility application UI that is Section 508-compliant. A Section 508-compliant application must meet the requirements set forth under Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 749(d)). ▪ *Review Standard*: The Auditor must confirm that EDE Entity's application meets the requirements set forth under Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 749(d)). The Auditor must verify and certify the following: – Within the Business Requirements Audit Report Template, the Auditor must confirm that the EDE Entity's application UI is Section 508-compliant. No specific report or supplemental documentation is required. – The Auditor may review results produced by a 508 compliance testing tool. If an EDE Entity uses a 508 compliance testing tool to verify that its UI is 508-compliant, its Auditor must, at a minimum, review the results produced by the testing tool and document any non-compliance, as well as any mitigation or remediation to address the non-compliance. It is not sufficient for an Auditor to state that an EDE Entity complies with the 508-Compliant UI requirement by confirming that the EDE Entity utilized a 508 compliance testing tool.
Non-English-language Version of the Application UI and Communication Materials	▪ *Requirement*: In accordance with 45 C.F.R. § 155.205(c)(2)(iv)(B) and (C), QHP issuers and web-brokers, including those that are EDE Entities, must translate applicable website content (e.g., the application UI) on Consumer-facing websites into any non-English language that is spoken by a limited English proficient (LEP) population that reaches 10 percent or more of the population of the relevant state, as determined in current guidance published by the Secretary of HHS.[12] EDE Entities must also translate communications informing Consumers of the availability of Exchange-generated EDNs; critical communications that the Consumer will no longer receive from the Exchange (to be identified by CMS); and any other critical communications that an EDE Entity is providing to the Consumer in relation to the Consumer's use of its EDE environment into any non-English language that is spoken by an LEP population that reaches 10 percent or more of the population of the relevant state, as determined in guidance published by the Secretary of HHS.[13] ▪ *Review Standard*: The Auditor must verify and certify the following: – The Auditor must confirm that the non-English-language version of the application UI and associated critical communications are compliant with the FFE requirements, including the Application UI Toolkit and Communications Toolkit. – The Auditor must verify that the application UI has the same meaning as its English-language version. – The Auditor must also verify that EDE Entity has met all EDE communications translation requirements released by CMS in the Communications Toolkit. – The Auditor must document compliance with this requirement within the Business Requirements Audit Report Template, the Application UI Toolkit, and the Communications Toolkit. In the toolkits, the Auditor can add additional columns for the Auditor compliance findings fields (yellow-shaded columns) or complete the Spanish audit in a second copy of each of the two toolkits.

[12] Guidance and Population Data for Exchanges, Qualified Health Plan Issuers, and Web-Brokers to Ensure Meaningful Access by Limited-English Proficient Speakers Under 45 CFR §155.205(c) and §156.250 (March 30, 2016) https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Language-access-guidance.pdf and "Appendix A- Top 15 Non-English Languages by State" https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Appendix-A-Top-15-non-english-by-state-MM-508_update12-20-16.pdf.

[13] *Frequently Asked Questions (FAQs) Regarding Spanish Translation and Audit Requirements for Enhanced Direct Enrollment (EDE) Entities Serving Consumers in States with FFEs* (June 20, 2018) provides further information regarding translation and audit requirements: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/FAQ-EDE-Spanish-Translation-and-Audit-Requirements.PDF.

Review Category	Requirement and Audit Standard
Agent and Broker Identity Proofing Verification	▪ *Requirement:* Agent/Broker Identity Proofing Requirements. EDE Entity must implement Agent and Broker identity verification procedures that consist of the following requirements: – EDE Entity must provide User-Id of the requester in the header for each EDE API call. For Agents and Brokers, the User-Id must exactly match the FFE-assigned User-Id for the Agent or Broker, or the request will fail FFE User-Id validation. For Consumers, the User-Id should be the User-Id for the Consumer 's account on the EDE Entity's site, or some other distinct identifier the EDE Entity assigns to for the Consumer. o If an EDE Entity is using the Fetch Eligibility API, the same User ID requirements apply. However, instead of sending the User ID via the header, the User ID will be provided in the request body via the following path: ExchangeUser/ExchangeUserIdentification/IdentificationID. – EDE Entity must identity proof all Agents and Brokers prior to allowing the Agents and Brokers to use its EDE environment. EDE Entity may conduct identity proofing in one of the following ways: – Use the FFE-provided Remote Identity Proofing/Fraud Solutions Archive Reporting Service (RIDP/FARS) APIs to remotely identity proof Agents and Brokers; OR – Manually identity proof Agents and Brokers following the guidelines outlined in the document "Acceptable Documentation for Identity Proofing" available on CMS zONE EDE Documents and Materials webpage (https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials). – EDE Entity must validate an Agent's or Broker's National Producer Number (NPN) using the National Insurance Producer Registry (https://www.nipr.com) prior to allowing the Agent or Broker to use its EDE environment. ▪ *Review Standard:* For audits submitted during plan year 2019, for verification of these procedures, the Auditor must verify and certify the following: – EDE Entity's inclusion of the appropriate Agent/Broker and Consumer User-Id fields in the EDE and Fetch Eligibility API calls. – EDE Entity's process for identity proofing an Agent or Broker prior to allowing an Agent or Broker to use its EDE environment. – EDE Entity's process for validating an Agent's or Broker's NPN using the National Insurance Producer Registry prior to allowing an Agent or Broker to use its EDE environment.

A. Audit Documentation

i. Required Business Audit Documentation

Exhibit 4 contains the required information that prospective EDE Entities must submit to CMS as part of the Business Audit to be approved to participate in EDE. CMS encourages prospective EDE Entities to use this table as a checklist to ensure they have met all requirements. Note: CMS may require prospective EDE Entities and/or their Auditors to submit additional documents and information at CMS' discretion.

Exhibit 4: Required Information for Business Audit

Document	Description	Submission Requirements	Entity Responsible (Upstream/Primary/ Both Primary and Upstream/Auditor)	Deadline
Notice of Intent to Participate and Auditor Confirmation	▪ Once the prospective EDE Entity has a confirmed Auditor(s) who will be completing its audit(s), it must notify CMS that it intends to apply to use the EDE pathway for PY 2019 or PY 2020 *prior to initiating the audit.* The email must include the following: – 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 – CMS-issued Hub Partner ID	▪ The QHP issuer or web-broker should email directenrollment@cms.hhs.gov ▪ Subject line should state: "Enhanced DE: Intent."	Primary	February 28, 2019
Confirmation of Upstream Entities	▪ CMS requires confirmation of any upstream EDE Entities that will use a primary EDE Entity's environment from both the primary and each upstream EDE Entity. ▪ *For upstream EDE Entities*: The email from the upstream EDE Entity must include the following: – Name of EDE Entity providing your EDE environment – Primary POC name, email, and phone number – Emergency POC name, email, and phone number	▪ The QHP issuer or web-broker should submit the documentation through the secure portal as part of the audit submission package, or subsequently if the upstream relationship is established after the audit submission to the DE Help Desk directenrollment@cms.hhs.gov.	Both Primary and Upstream	If known, primary EDE Entities will notify CMS as part of the audit submission. After audit submission, CMS will review and approve upstream EDE Entities on a rolling basis.

Document	Description	Submission Requirements	Entity Responsible (Upstream/Primary/ Both Primary and Upstream/Auditor)	Deadline
Privacy Questionnaire (or attestation, if applicable, see Submission Requirements)	▪ CMS will provide the questionnaire to each prospective EDE Entity as part of the audit submission package. ▪ If a prospective EDE Entity submitted a questionnaire during a prior application process, the Entity may submit an attestation if the responses to the privacy questionnaire will remain unchanged from the language already submitted to CMS.	▪ Submit via the secure portal ▪ If an EDE Entity submitted a questionnaire during a prior application process, the Entity may submit an attestation if the responses to the privacy questionnaire will remain unchanged from the language already submitted to CMS.	Primary	Submitted with audit submission, or no later than June 30, 2019.
Entity's website privacy policy statement(s) and Terms of Service (or attestation, if applicable; see Submission Requirements)	▪ Submit the URL and text of each privacy policy statement displayed on your website and your website's Terms of Service in a Microsoft Word document or a PDF.	▪ Submit via the secure portal ▪ If an EDE Entity was previously approved to use EDE, the Entity may submit an attestation if the privacy policy statement(s) and Terms of Service will remain unchanged from the language previously submitted to CMS.	Both Primary and Upstream	Submitted with Audit Submission, or no later than June 30, 2019.
Training	▪ Prospective EDE Entities and Auditors must complete the trainings outlined in Section VIII. The trainings are located on REGTAP (located at the following link: https://www.regtap.info/).	▪ The person taking the training must complete the course conclusion pages at the end of each module. ▪ The prospective EDE Entity and Auditor are NOT required to submit anything additional to CMS but must print a copy of the training confirmation webpage to provide to CMS, if requested.	Primary, Auditor CMS recommends that representatives from any upstream EDE Entities take the trainings outlined in Section VIII.	Trainings must be completed by Primary prospective EDE Entities and Auditors prior to Audit Submission

Document	Description	Submission Requirements	Entity Responsible (Upstream/Primary/ Both Primary and Upstream/Auditor)	Deadline
EDE Business Agreement	▪ Primary and upstream EDE Entities must submit the EDE Business Agreement to use the EDE pathway. The agreement must identify the Entity's selected Auditor. ▪ CMS will countersign the EDE Business Agreement after CMS has reviewed and approved the business requirements audit and the privacy and security audit.	▪ Submit via the secure portal	Both Primary and Upstream	Submitted with Audit Submission, or no later than June 30, 2019.
Business Audit Report and Toolkits	▪ A prospective EDE Entity must submit the Business Requirements Audit Report Template and all applicable toolkits completed by its Auditor. ▪ See below "Business Requirements Audit Resources" for more information.	▪ A prospective EDE Entity and its Auditor must submit the different parts of the Auditor resources package via the secure portal.	Primary	April 1, 2019–June 30, 2019
HUB Onboarding Form (for primary EDE Entities with upstream EDE Entities only)	▪ An EDE Entity that has upstream EDE Entities must provide a HUB Onboarding Form to CMS detailing the information to acquire Partner IDs for all upstream EDE Entities.	▪ Follow instructions on form (located at the following link: https://zone.cms.gov/document/hub-onboarding-form)	Primary	As upstream EDE Entities are added

ii. Business Requirements Audit Resources

CMS has provided the following resources and templates for Auditors to review and/or complete as part of each audit. The resources are available on CMS zONE.[14]

CMS will provide an Auditor resources package that will contain the following:

- *Business Requirements Audit Report Template:* The template will provide an outline and instructions for the contents of the business requirements audit report. Auditors will use this template to document a prospective EDE Entity's compliance with all business requirements, including those that the Auditor has reviewed using CMS-provided toolkits. Auditors must carefully review the instructions in the EDE Business Audit Instructions and Report Template.

[14] EDE documents and materials will be posted at the following link on CMS zONE: https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials.

- *Toolkits*: The Auditor resources package will contain multiple toolkits, each of which will correspond with one or more of the business requirements set forth in Exhibit 3. Each toolkit will provide testing scenarios that the Auditor will use to verify the prospective EDE Entity's compliance with the corresponding requirement(s). Each toolkit will contain a template that lists each scenario or requirement and provides a space for the Auditor to indicate the prospective EDE Entity's compliance. The prospective EDE Entity must submit the completed templates to CMS as part of the business requirements audit package. CMS will provide toolkits for the Eligibility Results Testing, API Functional Integration Testing, Application UI, and Consumer Communications requirements.
  - **Note:** The Auditor must not modify or delete any language provided in any toolkit or template.
  - **Note Regarding Phase-specific Requirements:** The Application UI and Eligibility Results Toolkits contain phase-specific requirements throughout the toolkits. Auditors and prospective EDE Entities must carefully review the **Instructions** tabs of these toolkits for information on how to identify the phase-specific requirements within the toolkits.

As of January 2019, the Auditor resources package is a zip file that contains, at a high level, the following files for Auditors and prospective EDE Entities to reference:

1. EDE Business Audit Instructions and Report Template
2. Application User Interface (UI) Toolkit
3. EDE End-to-End Test Data (used as part of the API Functional Integration Toolkit)
4. EDE Eligibility Results Toolkits (three phase-specific versions)
   - Eligibility Results Toolkit - Phase 1 – PY 2019
   - Eligibility Results Toolkit - Phase 2 – PY 2019
   - Eligibility Results Toolkit - Phase 3 – PY 2019
5. Communications Toolkit
6. API Functional Integration Toolkit
7. Communications Supplemental Content (English)
8. Communications Supplemental Content (Spanish)
9. Application Supplemental Content
   - FY18 Q2 FFM State Configuration for EDE Review

VII. Privacy and Security Audit Requirements and Scope

An Auditor must complete the Security and Privacy Controls Assessment Test Plan (SAP), which must be submitted to CMS for review prior to initiating the Security and Privacy Controls Assessment (SCA) portion of the audit. The Auditor will complete a privacy and security audit to ensure that the prospective EDE Entity complies with applicable requirements as defined in CMS regulations and this guidance. A prospective EDE Entity must submit the resulting privacy and security audit package to CMS. Exhibit 5 describes the review areas and review standards for the privacy and security requirements.

Exhibit 5. Privacy and Security Requirements

Review Category	Audit Standards
Privacy and Security Control Implementation	▪ *Requirement:* An EDE Entity must implement security and privacy controls, a fully completed SSP, as well as other privacy and security standards, for protecting the confidentiality, integrity, and availability of the information collected, used, disclosed, and/or retained by the EDE Entity as defined in the ISA and EDE Business Agreement prior to conducting the privacy and security audits. ▪ *Review Standard*: The Auditor must conduct a Security and Privacy Control Assessment (SCA) and produce a SAR to certify that the EDE Entity has implemented processes sufficient to meet the privacy and security requirements set forth in the ISA and EDE Business Agreement and in applicable regulations. ▪ If the Auditor determines that the EDE Entity does not meet one or more privacy and security requirements, the EDE Entity must create a plan of action and milestones (POA&M) to resolve the deficiency. The POA&M should include a corrective action plan that explains how the EDE Entity will come into compliance with each requirement and will state the estimated completion date for each identified milestone. Monthly reviews and updates are required to be submitted to CMS until all significant findings are resolved based on findings from SCAs, security impact analyses, and continuous monitoring activities outlined in the ISCM Strategy Guide. Auditors must verify that the EDE Entity's website complies with the privacy and security standards, and that the website is consistent with third-party data collection tools and standards to be defined by CMS in subsequent guidance; CMS regulations; and subsequent technical, and training documents. Additional information can be found in the EDE Privacy/Security Standards training module.

A. *Audit Documentation*

i. *Required Privacy and Security Audit Documentation*

The table below contains the required information that primary prospective EDE Entities must submit to CMS as part of its Privacy and Security Audit to be approved to participate in EDE.

Exhibit 6: Privacy and Security Audit Information Requirements

Document	Description	Submission Requirements	Deadline
Interconnection Security Agreement (ISA)	▪ A prospective 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.	▪ A prospective EDE Entity must submit the ISA via the secure portal.	▪ April 1, 2019–June 30, 2019
Security Privacy Controls Assessment Test Plan (SAP)	▪ This report is to be completed by the Auditor and submitted to CMS prior to the audit. ▪ The SAP describes the Auditor's scope and methodology of the assessment. The SAP includes an attestation of the Auditor's independence.	▪ A prospective EDE Entity and its Auditor must submit the SAP completed by its Auditor.	▪ Before commencing the privacy and security audit; during a prospective EDE Entity and the Auditor planning phase
Security Privacy Assessment Report (SAR)	▪ This report details the Auditor's assessment findings of the prospective EDE Entity's security and privacy controls implementation.	▪ A prospective EDE Entity and its Auditor must submit the SAR completed by its Auditor via the secure portal.	▪ April 1, 2019–June 30, 2019

Document	Description	Submission Requirements	Deadline
Plan of Actions & Milestones (POA&M)	▪ A prospective EDE Entity must submit a POA&M if its Auditor identifies any privacy and security compliance issues in the SAR. ▪ The POA&M details a corrective action plan and the estimated completion date for identified milestones.	▪ A prospective EDE Entity and its Auditor must submit the POA&M in conjunction with the SAR via the secure portal. ▪ POA&Ms with outstanding findings must be submitted monthly to CMS until all significant vulnerabilities are addressed. The POA&M must be submitted quarterly thereafter.	▪ April 1, 2019–June 30, 2019
Privacy Impact Assessment (PIA)	▪ The PIA will detail the prospective EDE Entity's evaluation of its controls for protecting PII.	▪ A prospective EDE Entity is not required to submit the PIA to CMS. However, per the ISA, CMS may request and review an EDE Entity's PIA at any time, including for audit purposes.	▪ Before commencing the privacy and security audit as part of the EDE SSP
System Security and Privacy Plan (SSP)	▪ The SSP will include detailed information about the prospective EDE Entity's implementation of required security and privacy controls.	▪ A prospective EDE Entity is not required to submit the SSP to CMS. However, per the ISA, CMS may request and review an EDE Entity's SSP at any time, including for audit purposes. ▪ The implementation of security and privacy controls must be completely documented in the SSP before the audit is initiated.	▪ Before commencing the privacy and security audit
Incident Response Plan and Incident/Breach Notification Plan	▪ A prospective EDE Entity is required to implement breach and incident handling procedures that are consistent with CMS' Incident and Breach Notification Procedures. ▪ A prospective EDE Entity must incorporate these procedures into its own written policies and procedures.[15]	▪ A prospective EDE Entity is not required to submit the Incident Response Plan and Incident/Breach Notification Plan to CMS. However, per the ISA, CMS may request and review an EDE Entity's Incident Response Plan and Incident/Breach Notification Plan at any time, including for audit purposes.	▪ Before commencing the privacy and security audit as part of the EDE SSP
Vulnerability Scan	▪ A prospective EDE Entity is required to conduct monthly Vulnerability Scans.	▪ A prospective EDE Entity and its Auditor must submit the last three months of their Vulnerability Scan Reports, in conjunction with POA&M and SAR via the secure portal.	▪ April 1, 2019–June 30, 2019

[15] https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-08-Incident-Response.pdf.

ii. Privacy and Security Audit Resources

CMS will provide the following resources and templates for Auditors to review and/or complete as part of each ORR audit. The resources will be available on CMS zONE.[16]

CMS will provide an Auditor resources package that will contain the following:

- **Framework for the Independent Assessment of Security and Privacy Controls (Framework):** The Framework will provide an overview of the independent security and privacy assessment requirements. The Auditor should review the Framework prior to conducting the privacy and security audit.
- **System Security and Privacy Plan (SSP) Workbook and Final SSP:** The prospective EDE Entity will use the SSP Workbook to create a final SSP, which will include detailed information about the prospective EDE Entity's implementation of security and privacy controls. The Auditor will review the SSP Workbook and final SSP to make its assessment of the prospective EDE Entity's compliance with the required privacy and security controls.
- **Security and Privacy Controls Assessment Test Plan (SAP) Template:** The SAP will contain a high-level description of the critical items that the Auditor must test. The Auditor and the prospective EDE Entity must supply this document and submit it to CMS for review prior to conducting the privacy and security audit.
- **Security & Privacy Assessment Report (SAR) Template:** The Auditor is required to use this template to document the audit findings on whether or not the prospective EDE Entity has implemented the required privacy and security controls correctly.
- **Plan of Action and Milestones (POA&M) Template:** The prospective EDE Entity will be required to use this template to create a POA&M. The POA&M entries are created within thirty (30) days of the final results for every internal/external audit/review or test (e.g., security controls assessment, penetration test) to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security and privacy controls and to reduce or eliminate known vulnerabilities. The POA&Ms should be submitted to CMS monthly until all significant vulnerabilities are remediated.
- **Information Security and Privacy Continuous Monitoring (ISCM) Strategy Guide:** The ISCM Strategy Guide provides the minimum requirements for an EDE Entity to implement an ISCM program for its systems and to maintain ongoing CMS authorization and approval. ISCM provides a mechanism for an 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. 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.

[16] EDE documents and materials will be posted at the following link on CMS zONE: https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials.

VIII. Required Auditor and Prospective EDE Entity Training

The Auditor(s) selected by the prospective EDE Entity and representative(s) from the prospective EDE Entity are required to take CMS-mandated training, as summarized in Exhibit 7.

Exhibit 7: Auditor and Prospective EDE Entity Training

Business Requirements Auditor Training Requirement	Privacy and Security Auditor Training Requirement	Prospective EDE Entity 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 UI Services, and - Other potential modules to be defined by CMS.	• 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.	• 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.

All Auditor representatives responsible for conducting the business requirements audit and/or the privacy and security audit must take the required trainings relevant to the audit(s) they are conducting. The same individual from each Entity does not need to complete all trainings; in this situation, CMS expects that an individual would take the training most suited to the individual's role in conducting the audit or implementing the EDE environment.

The training is a self-paced computer-based training (CBT) and provides information about compliance, EDE technical requirements, privacy and security, and reporting requirements. CMS will release further information regarding the training via REGTAP and anticipates the trainings will become available beginning in early 2019. All training modules will be posted on REGTAP as they become available.[17]

Trainings from the PY 2019 OEP approval process are still available on REGTAP; however, CMS will release updates to these modules in early 2019 for Auditors and prospective EDE Entities to take the revised modules. Prospective EDE Entities and their Auditors may take the PY 2019 trainings that currently exist on REGTAP prior to starting the audit instead of waiting for the updated PY 2020 trainings. Prospective EDE Entities and their Auditors who use this option may need to take the updated PY 2020 trainings prior to submitting the audit. If the PY 2020 training is required, EDE Entities and their Auditors will be accountable for any updates in the PY 2020 training if they take this approach (i.e., they take the PY 2019 training first). CMS

[17] REGTAP can be accessed at the following link: https://www.regtap.info/.

will indicate which revised modules must be taken by prospective EDE Entities and their Auditors as the modules are released.

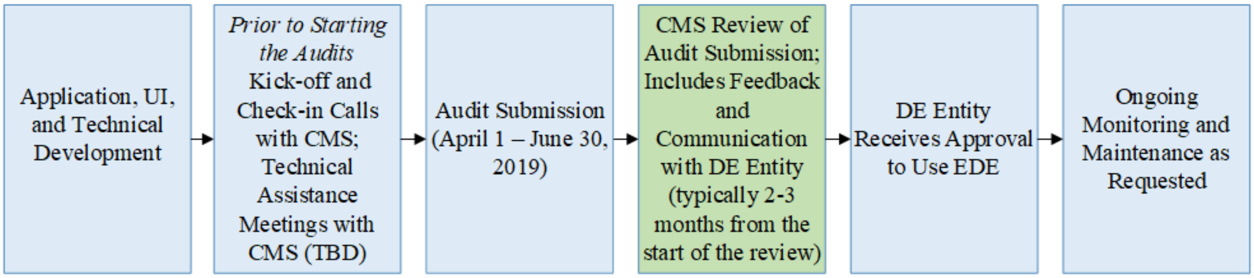
IX. Secure Portal for Document Submission

CMS will require a prospective EDE Entity to submit documents to CMS via a secure portal. After the Entity informs CMS that it has entered into an agreement with its Auditor(s), CMS will provide the Entity with instructions to establish an account on the secure portal that the Entity will use to access and upload documents to the portal. CMS will also provide written instructions for using the secure portal via email at that time. CMS will not require prospective EDE Entities to encrypt documents containing proprietary information before uploading them to the portal.

X. Approval Process and Audit Submission Window

As shown in Exhibit 8, the EDE approval process consists of several phases. Additional information is provided below.

Exhibit 8: Audit Submission and Approval Phases Overview


Application, UI, and Technical Development
Prior to Starting the Audits Kick-off and Check-in Calls with CMS; Technical Assistance Meetings with CMS (TBD)
Audit Submission (April 1 – June 30, 2019)
CMS Review of Audit Submission; Includes Feedback and Communication with DE Entity (typically 2-3 months from the start of the review)
DE Entity Receives Approval to Use EDE
Ongoing Monitoring and Maintenance as Requested

A. Pre-Audit Notification to CMS

Once a prospective EDE Entity has contracted with an Auditor(s) to complete the two parts of the ORR, the Entity's privacy and security Auditor must complete the SAP. This must be submitted to CMS for review prior to conducting the privacy and security audit. The Entity must notify the DE Help Desk before its Auditor begins its audit (at least one to two 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.

B. Audit Submission Deadlines

Prospective EDE Entities interested in implementing EDE in calendar year 2019 must submit business requirements and privacy and security audits during the audit submission window from April 1, 2019–June 30, 2019. CMS will not accept audits received outside of this submission window. There is no guarantee that every prospective EDE Entity that submits an audit in the submission window will receive approval to go live with EDE before the start of the PY 2020 Open Enrollment Period or even during calendar year 2019.

If a prospective EDE Entity submits an audit, and then resubmits its audit before receiving feedback from CMS, 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 submitted.

If a prospective EDE Entity or an EDE Entity changing phases intends to submit its audit during the April 1, 2019–June 30, 2019 submission window, it must submit its notice of intent to directenrollment@cms.hhs.gov by February 28, 2019, or as soon as possible. If an Entity submits an incomplete audit, once the Entity resubmits its audit, CMS will prioritize that resubmitted audit at the end of the review queue. CMS does not guarantee any approval timelines.

CMS expects to issue updated requirements, trainings (required for both Auditors and representatives of prospective EDE Entities), agreements, and baseline toolkits for the April 1, 2019–June 30, 2019 submission window in early 2019. CMS expects to primarily use the same content as the materials released in 2018 for PY 2019. Accordingly, prospective EDE Entities can begin developing their EDE environments based on the existing toolkits and privacy and security documentation that are located on CMS zONE.[18]

Prospective EDE Entities that submit complete audits early in the April 1, 2019–June 30, 2019 submission window will receive the opportunity to have additional technical assistance calls with CMS and expedited audit submission review.

C. Completeness Requirements

i. Submitting a Complete Business Requirements Audit

CMS will review each audit submission for completeness. CMS will not accept incomplete audits. A complete business requirements audit submission meets the criteria described in Exhibit 9, at a minimum.

Exhibit 9: Business Requirements Audit Submission Requirements for a Complete Audit

Toolkit & Template	Minimum Requirements for a Complete Audit
All Toolkits	▪ Provide 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 test cases in the Eligibility Results Toolkits do not cover all questions in the Application UI Toolkit.
Eligibility Results Toolkit(s)	▪ Screenshots of the entire application flow are provided for each test case. ▪ Correct eligibility results and eligibility determination notices (EDNs) are provided for each test case.
API Functional Integration Toolkit	▪ Correct results and successful completion of each test case is documented.

[18] EDE documents and materials will be posted at the following link on CMS zONE: https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials. Note that prospective EDE Entities must set up a CMS Enterprise Portal account and request zONE access to view the zONE website. 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.

Toolkit & Template	Minimum Requirements for a Complete Audit
EDE Business Audit Report Template	▪ Complete descriptions of each requirement; Auditors must not exclude key aspects of each requirement
Supplemental Documentation	▪ 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 Report or toolkits.

An incomplete business requirements audit is an audit that does not meet the criteria described above. The Auditor must take the appropriate actions to complete the incomplete audit and the prospective EDE Entity must resubmit it, as applicable.

CMS will conduct an initial high-level review of all audit submissions in the order they are received and based on available resources. 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. 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.

Audits should not include comments that describe the Auditor'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.

ii. Submitting a Complete Privacy and Security Audit

CMS will review each audit submission for completeness. CMS will not accept incomplete audits. A complete security audit submission meets the criteria described in Exhibit 10, at a minimum.

Exhibit 10: Privacy and Security Audit Submission Requirements for a Complete Audit

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.

Document	Minimum Requirements for a Complete Audit
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.
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 is an audit that does not meet the criteria described above. The Auditor must take the appropriate actions to complete the incomplete audit and the prospective EDE Entity must resubmit it, as applicable. Prospective EDE Entities with incomplete audits must resubmit complete audits and will not be reviewed further until complete audits have been submitted.

D. Business Requirements Audit-specific Requirements

i. Application Technical Assistance Process

Prior to conducting and submitting an audit, a prospective EDE Entity can request feedback from CMS on its planned application UI build. Regardless of whether a prospective EDE Entity requests feedback from CMS, all prospective EDE Entities must provide testing environment credentials. The technical assistance process described in this section is a separate process from the audit review and mini audit process described later. Please note, an initial meeting between CMS and each prospective EDE Entity's Auditor is required as described in Section X.A.

Regarding technical assistance, a prospective EDE Entity can submit a request for CMS' application UI feedback with the relevant screenshots or testing environment credentials through the secure portal. The purpose of this process is to answer clarifying questions about application requirements and help mitigate the risk that CMS identifies compliance issues during the CMS-conducted mini audit (discussed in Section X.E, Enhanced DE Oversight, of these guidelines). Requests should contain specific questions related to UI development such as policy guidance, application requirements and flexibilities, technical design, and high-level application requirements and flow. The prospective EDE Entity should not request approval for unique variations that fall outside of the requirements and flexibilities provided by CMS, as these will not be approved.

A prospective EDE Entity may submit application UI feedback requests up until the completion of the business requirements audit; upon submission of the audit, the prospective EDE Entity's application should be finalized. If CMS determines a discussion with the prospective EDE Entity and/or Auditor is needed, CMS will schedule a meeting between the prospective EDE Entity, the Entity's CMS Direct Enrollment Point of Contact (DEPOC), and the appropriate CMS subject matter experts (SMEs).

CMS may release updated application guidance based on feedback received. While CMS may provide feedback to prospective EDE Entities on the application and UI, the Entity's Auditor should still include a compliance determination with respect to all requirements consistent with these guidelines and other guidance.

E. Enhanced DE Oversight

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. 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. The prospective EDE Entity will be required to provide CMS, via the DE Help Desk, with a set of credentials that CMS can use to access the Entity's testing environment (i.e., pre-production environment) to complete the mini audit of the Entity's EDE 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. The prospective EDE Entity must not make changes to its EDE environment after submitting its audit package, unless instructed by CMS or following the partner-initiated CR protocol.

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.

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 (see Section XI, Processes for Changes to an Audited or Approved EDE Environment) in an EDE Entity's EDE environment.

F. Final Approval Process

CMS will review and approve prospective EDE Entities to use the EDE pathway on a first-come, first-served basis once the Entities submit a complete audit (as defined above). Prospective EDE Entities must submit their documentation no later than June 30, 2019 for their audit to be reviewed and potentially approved before the 2020 OEP. CMS encourages prospective EDE Entities to submit as early as possible in the audit submission window (but no earlier than April 1, 2019); however, prospective EDE Entities should *not* submit incomplete audits or audits with material deficiencies. CMS strongly encourages each prospective EDE Entity to request technical assistance from CMS per the process defined above for the prospective EDE Entity's proposed application UI. All prospective EDE Entities must provide testing environment credentials as part of the approval process as described in Sections X.D and X.E.

CMS will notify prospective EDE Entities on a rolling basis of approval to use the EDE pathway. Prospective EDE Entities may not be approved in the order in which their audits were submitted because the content and quality of the audit submissions vary substantially and that affects the amount of time it takes to review. CMS will countersign a prospective EDE Entity's EDE Business Agreement and ISA after CMS reviews and approves the Entity's business audit package and privacy and security audit package, and after it confirms that the Entity's EDE environment is functional. After CMS countersigns the EDE Business Agreement and the ISA, CMS will inform the Entity of the subsequent steps to connect its EDE environment to the EDE pathway.

XI. Processes for Changes to an Audited or Approved EDE Environment

A. EDE Entity-initiated EDE Phase Change Requests

i. Business Audit Requirements

If an EDE Entity opts to change to a different EDE application phase (from its approved or audited EDE phase), the Auditor must conduct portions of a revised business requirements audit to account for the changes to the EDE Entity's EDE environment necessary to implement the newly selected phase and to confirm compliance with all applicable EDE requirements. CMS will review business requirements audit submissions for new phases as if they were initial audit submissions. Any audit submissions must be received during an audit submission window as described previously.

Exhibit 11 indicates the required materials an EDE Entity must have an Auditor complete for an EDE Entity to transition to a new application phase for the business requirements audit.

Exhibit 11: Business Audit Phase Change Requirements

Business Audit Documentation	Business Audit Phase Change Requirements
Business Audit Report	For all phase CRs, the EDE Entity's Auditor must document compliance with the following sections of the Business Audit Report (and the associated toolkits): ▪ Review Category 1 ▪ Review Category 2 ▪ Review Category 3 ▪ Review Category 4 ▪ Review Category 5 (if applicable) ▪ Review Category 6 ▪ Review Category 7 ▪ Review Category 10 ▪ Review Category 11 (if applicable)
Application UI Toolkit	For all phase CRs, the EDE Entity's Auditor must complete the entirety of the Application UI Toolkit for the EDE Entity's new phase. This includes the screening questions tabs (for Phase 1 or Phase 2 EDE Entities only), the UI Questions tab, the High-Level Requirements tab, and the Eligibility Results tab.
Eligibility Results Toolkit	For all phase CRs, the EDE Entity's Auditor must complete all of the relevant test cases for the applicable EDE Entity's phase. For example, if an EDE Entity is changing to Phase 3, the Auditor must complete and submit evidence for all test cases, as noted in the "Auditor User Guide" tab, including the applicable test cases in the Phase 1 and Phase 2 Eligibility Results Toolkits.
Communications Toolkit	For phase changes to phase 3 or down from phase 3, the EDE Entity's Auditor must re-evaluate the compliance of the "Phase-specific Requirements" requirement in the Communications Toolkit (row 5 of the baseline toolkit from plan year 2019).
API Functional Integration Toolkit	For all phase CRs, the EDE Entity's Auditor must complete all test cases within the API Functional Integration Toolkit.

ii. Privacy and Security Audit Requirements

EDE Entities will not need to submit additional privacy and security documentation specifically for an EDE application phase change.

B. CMS-initiated Change Requests

i. CMS-initiated Change Request Process

CMS will periodically release updates to EDE program requirements in the form of CMS-initiated CRs. Usually, these changes will take the form of an update to one of the business report toolkits. CMS may require EDE Entities to implement new or updated EDE requirements, including updates to business requirements audit toolkit versions that are released after the date of the CMS-designated baseline version of each toolkit. These required revisions will be considered CMS-initiated CRs.

EDE Entities have two options to implement required revisions:

- Submit supplemental documentation; or

- Have their Auditor review the required revision as part of the business requirements audit. For example, if the required revision is in a toolkit, the Auditor will use the version of the toolkit containing the revision(s) to complete the business requirements audit.
    - **Note:** The EDE Change Request Tracker is stored on CMS zONE;[19] accordingly, Auditors do not have access to the EDE Change Request Tracker. EDE Entities must provide a copy of the Change Request Tracker to their Auditor(s).

All EDE Entities participating in EDE must implement CMS-initiated CRs. However, depending on when an EDE Entity submits its business requirements audit in relation to when CMS notifies EDE Entities about a required CR, the CR may be audited as part of the business requirements audit or the EDE Entity may demonstrate that it has implemented the CR as part of a separate process. Specifically:

- EDE Entities that have already submitted their business requirements audit before the CR is released must submit evidence of their implementation of the CR in clearly labeled supplemental documentation, rather than have their Auditor re-review the portion of the audit affected by the CR.
- EDE Entities that submit their audits after the CR is released, but before the implementation deadline have two options: (1) they may have their Auditor review the CR as part of the business requirements audit or (2) they may provide clearly labeled supplemental documentation of their implementation of the CR anytime up until the implementation deadline stated in the EDE Change Request Tracker (explained below).
- EDE Entities that submit their audits after the CR implementation deadline will be required to submit documentation of their implementation of the CR with their audit submission (either incorporated in the Auditor's review or in clearly labeled supplemental documentation).

ii. CMS Change Request Tracker

CMS will specify the changes that EDE Entities are required to implement via the EDE Change Request Tracker, which is posted on the EDE Documents and Materials page on CMS zONE.[20]

The EDE Change Request Tracker is a spreadsheet containing information about each CMS-initiated CR, including a description of each CR; the EDE document in which the CR appears; whether the EDE Entity must submit documentation to demonstrate compliance and, if so, the type of documentation the EDE Entity must submit (e.g., if EDE Entities must submit screenshots or some other type of evidence of implementation); the deadline for submission of documentation; the method of submission of required documentation; and conditional requirements, if applicable. The Change Request Tracker only describes the CR; the EDE Entity must review the CR within the identified EDE document.

[19] EDE documents and materials will be posted at the following link on CMS zONE: https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials.

[20] EDE documents and materials will be posted at the following link on CMS zONE: https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials.

iii. Deadlines for Implementation of Required Changes and Potential Penalties

CMS will attempt to provide as much notice to EDE Entities as feasible regarding CMS-initiated CRs. Per the EDE Business Agreement, CMS will provide a timeline for each CMS-initiated CR for EDE Entities to implement the change. While CMS anticipates that this will be a rare occasion, some CMS-initiated CRs may require significant revisions to the EDE environment that would require independent verification by a third-party Auditor. CMS will attempt to provide more advance notice to EDE Entities in the event CMS requires a CMS-initiated CR of this type.

If an EDE Entity does not timely submit documentation of its implementation of such CRs, CMS may suspend the non-compliant EDE Entity's access to the EDE pathway. If an EDE Entity does not meet the deadline to provide evidence of implementation of the CR and has not already been approved to participate in EDE, the EDE Entity will not be approved until after the appropriate documentation is submitted.

iv. Implementation of Other Changes

CMS will periodically release updates to EDE documentation that are not included in the Change Request Tracker. These updates include clarifications, technical corrections, and content updates. These types of updates do not amount to changes in business requirements and accordingly will not be communicated through the Change Request Tracker. Instead, these changes will be noted through release of new versions of EDE documentation and communicated through EDE partner calls, e-blasts, and other technical assistance channels.

While proof of implementation is not required for this category of changes, EDE Entities are strongly encouraged to pay close attention to and implement these updates where appropriate, as failure to do so may result in validation or other errors or have other adverse impacts on an EDE Entity's environment.

C. Other EDE Entity-initiated Change Requests

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 in this section. This process is specific to other EDE Entity-initiated changes and does not include EDE-Entity initiated phase CRs (Section XI.A, EDE Entity-initiated EDE Phase Change Requests above) or CMS-initiated CRs (Section XI.B, CMS-initiated Change Requests above). The EDE Entity must continue to comply with requirements of the configuration management control family as outlined in the Non-Exchange Entities (NEE) Security and Privacy Plan (SSP) workbook.[21] All changes must be tested, validated, and documented before implementing the changes in the operational system.

i. Change Categories

In Exhibit 12, CMS provides a categorization of the types of changes EDE Entities might make to their EDE environments with examples. The process for implementing a change within each category is provided below Exhibit 12. EDE Entities are not required to notify CMS of any changes made to their EDE environment that do not fall under the scope of one of the below

[21] The NEE SSP workbook is available on the EDE Documents and Materials webpage on CMS zONE: https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials.

change categories. Exhibit 12 is intended to serve as a guideline for EDE Entities; EDE Entities should contact the DE Help Desk (directenrollment@cms.hhs.gov) if they are unsure what category a change falls under.

Exhibit 12: Types of Changes EDE Entities Might Make to Their EDE Environments

Change Category	Brief Description	Examples of Changes in this Category
Category 1: Changes that require CMS notification, but that CMS does not need to approve	These changes include any system or software updates that do not alter the privacy and security status of the EDE environment as represented in the CMS-approved audit or changes to the EDE environment that have no effect on the consumer's UI experience. Can include significant changes in an Entity's communication strategy with consumers that don't impact the UI. These changes may also include modifications to the information presented to consumers, applicants, qualified individuals, or enrollees regarding eligibility, the eligibility application, the eligibility determination, and enrollment processes if CMS has previously messaged that it is a permissible change.	▪ System version updates ▪ Fixes to typos and other bugs ▪ Changes to design elements such as color, font, navigational menus, etc. ▪ Changes to EDE Entity branding or EDE Entity support channel contact information ▪ Addition of CMS-approved help text language provided in the Application UI Toolkit, Phase 1 Screening Questions, Phase 2 Screening Questions, and Phase 3 Screening Questions tabs under the column entitled "Question Help" and the UI Questions tab under the column entitled "Informational Text" ▪ Significant changes in how the Entity communicates with consumers on required actions and about new status information (i.e. communications about notices, data matching issue [DMI] deadlines, etc.) where a significant change in messaging (that CMS has messaged is permissible), frequency, or method is made. For example, changing email communications on DMI deadline reminders from once a week to daily, or stopping communications (emails, texts, calls) on something the consumer still needs to do.
Category 2: Changes that require CMS notification and pre-approval, with accompanying documentation	These changes include any modifications to the information presented to consumers, applicants, qualified individuals, or enrollees regarding eligibility, the eligibility application, the eligibility determination, enrollment processes, status, action items, and related communications about eligibility and enrollment. These changes do not include modifications to the information presented to consumers, applicants, qualified individuals, or enrollees regarding eligibility, the eligibility application, the eligibility determination, and enrollment processes if CMS has previously messaged that it is a permissible change (this falls within Change Category #1, as set forth above).	▪ Minor changes to the consumer's UI, including the application or enrollment experience, that go beyond the changes described above. For example, changes to the wording of a set of questions and answers not explicitly described in the UI Question Companion Guide, or changes to whether previously entered information is pre-populated when the applicant reports a life change. – Changes to the eligibility application that add or remove questions from displaying for any eligibility scenario. For example, adding a question or tool to help consumers calculate their projected annual income – Changes to the eligibility application that change the order of questions, or the conditional logic for when questions appear. For example, making a change to ask the Medicaid block questions after the income questions instead of before – Changes to account management capabilities (application and enrollment statuses, notices, consumer action items, etc.). For example, changes to the wording of a set of questions and answers or changes to how DMI and special enrollment period verification issue (SVI) status and notices are displayed and communicated to consumers

Change Category	Brief Description	Examples of Changes in this Category
Category 3: Changes that require CMS notification, pre-approval, and verification by an independent third-party Auditor	These changes include any modifications to the systems comprising the EDE environment to the extent that the CMS-approved audits and existing Interconnection Security Agreement (ISA) no longer accurately reflect the compliance of the environment.	▪ Adding new systems to the EDE environment ▪ Significant code changes[22] ▪ Moving to a new data center ▪ Altering the way consumers access the application (e.g., moving it from an internal system to an external system) ▪ Changes to the scenarios supported by the eligibility application or transition to a different eligibility application phase.

ii. Process for Implementation of Changes within Each Category

- **Change Category 1 – Changes that require CMS notification, but that CMS does not need to approve:**
  - EDE Entities must email the DE Help Desk (directenrollment@cms.hhs.gov) and detail the scope of the change. The email subject line must start with "Category 1 Change."
  - EDE Entities may submit accompanying documentation, but it is not required. EDE Entities should submit any accompanying documentation through the secure portal.
- **Change Category 2 – Changes that require CMS notification and pre-approval, with accompanying documentation:**
  - EDE Entities must email the DE Help Desk (directenrollment@cms.hhs.gov) and detail the scope of the change that they intend to make. The email subject line must start with "Category 2 Change."
  - EDE Entities must submit accompanying documentation through the secure portal. Examples of documentation include a mock-up of the UI or a screenshot from within the EDE Entity's testing environment that demonstrates the intended change.
  - This type of change requires pre-approval from CMS; CMS will review the change and respond to the EDE Entity. CMS cannot guarantee a response timeframe. CMS will either confirm that the EDE Entity can proceed or may request additional information.
- **Change Category 3 – Changes that require CMS notification, pre-approval, and verification by an independent third-party Auditor:**
  - EDE Entities must email the DE Help Desk (directenrollment@cms.hhs.gov) and detail the scope of the change that they intend to make, how the Auditor will review the change, and what documentation the Auditor will prepare. The email subject line

[22] Per National Institute of Standards and Technology (NIST) SP800-37, significant changes to an information system may include, for example: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls. Examples of significant changes to the environment of operations may include, for example: (i) moving to a new facility; (ii) adding new core missions or business functions; (iii) acquiring specific and credible threat information that the organization is being targeted by a threat source; or (iv) establishing new/modified laws, directives, policies, or regulations.

must start with "Category 3 Change." Examples of documentation prepared by the Auditor include an updated Plan of Action and Milestones (POA&M), updated toolkit, or an updated Security and Privacy Assessment Report (SAR). At this step, EDE Entities may submit accompanying documentation through the secure portal if it would be helpful for CMS review.

- The EDE Entity must email the request to CMS for pre-approval prior to implementing the change and having it verified by a third-party Auditor. CMS will review the change and respond to the EDE Entity. CMS cannot guarantee a response timeframe. CMS will either confirm that the EDE Entity can proceed or may request additional information.
- After the Auditor verifies the change, the EDE Entity must submit the documentation prepared by the Auditor (previously approved by CMS).

XII. Resources

A. Help Desk

In addition to hosting weekly webinars inclusive of interactive question and answers, CMS currently manages multiple EDE Entity-facing help desks to address questions; help EDE Entities and prospective EDE Entities resolve technical problems, operational issues, and other issues, and respond to policy questions. An Entity must either remove PII in documents before sending them to the help desks or encrypt the e-mail transmitting the PII.

- An EDE Entity with technical issues or questions that concern its 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 "EDE: Tech Q for [Partner] on [Topic]." An EDE Entity may also use the FEPS Help Desk to send technical questions asked by its Auditor(s).
- An EDE Entity with technical questions specifically related to Hub onboarding for EDE in general, Hub onboarding for the various EDE APIs, connectivity issues related to accessing the EDE APIs, or testing and production of RIDP/FARS may alternatively e-mail the Hub Help Desk at dsh.support@qssinc.com with the subject line "EDE: API Q for [Partner] on [Topic]." Emails to the FEPS Help Desk and Hub Help Desk will be routed to the appropriate EDE team.

For a timely response, the EDE Entity representative submitting the question should ensure that emails to the FEPS Help Desk and Hub Help Desk include the following information:

- Your contact information (e-mail and phone number).
- Name of your organization and either your organization's five-character Health Insurance Oversight System (HIOS) ID (if an existing issuer) or CMS-issued Partner ID (if an existing web-broker).
- At the top of your email, please summarize whether your e-mail concerns an EDE 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 email to the right SME for a more efficient response.

- If reporting on a technical issue you encounter in production or while testing EDE, please include the request/response XMLs/JSONs for troubleshooting (API requests and responses). EDE Entities must remove PII prior to sending the XML/JSON to the FEPS Help Desk or Hub Help Desk or the EDE Entity must encrypt the email.

An EDE Entity with a policy and compliance question related to the business requirements audit or EDE Business Agreement should email the DE Help Desk at directenrollment@cms.hhs.gov with the subject line “EDE: [Audit/Compliance] Q for [Partner] on [Topic].”

An EDE Entity with a policy and compliance question related to the privacy and security audit, privacy and security controls, or its ISA should email the DE Help Desk at directenrollment@cms.hhs.gov with the subject line “EDE: [Privacy/Security] Q for [Partner] on [Topic].”

CMS will summarize and share answers to frequently asked questions (FAQs) on EDE that are sent to the DE Help Desk on the CMS-Issuer Technical Work Group (ITWG) webinar, which is open to all issuers and web-brokers on Tuesday afternoons. Please see the Section XIIB, Webinars, for webinar details.

Questions related to policy or compliance issues for either the business requirements audit or the privacy and security audit must be sent to the DE Help Desk. CMS will not respond to policy questions on either of these topics if they are not sent to the DE Help Desk. If an EDE Entity has been assigned a DEPOC at CMS, it should copy its DEPOC on all emails it sends to the FEPS Help Desk, Hub Help Desk, and DE Help Desk.

B. Webinars

CMS presents important EDE updates through two main communication channels summarized in Exhibit 13. Further details are provided below.

Exhibit 13: EDE-Related Training Opportunities

Public Webinars

Estimated early 2019

Issuer Technical Workgroup (ITWG) Webinar

Weekly; EDE, and DE updates provided as needed

CMS will host several public webinars in early 2019. CMS anticipates that recordings of these webinars will be available. The purpose of the webinars will be to present the guidelines and to provide best practices for submitting both audits.

CMS currently hosts the 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 FFE or SBE-FPs. CMS will continue to use the ITWG call to update the DE/EDE community on developments related to EDE 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:

- Webinar Registration URL: One time registration at the URL below: (If you have already registered for this webinar series please use the login information sent to you by webex.com) https://meetings-cms.webex.com/meetings-cms/k2/j.php?MTID=t21678f1219cf290a1dc0e69b4dc59999

Additionally, as described in Section X.A, Pre-Audit Notification to CMS, CMS will hold one-on-one informational discussions with an EDE Entity and its Auditor prior to the Auditor initiating the EDE audits. The purpose of this discussion is to answer questions and provide EDE best practices.

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, audit resources, and other documentation on the CMS zONE EDE Documents and Materials webpage.[23]

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 EDE updates, information for third-party Auditors, webinar slide decks, and FAQs to these communities, and will highlight updates during the weekly ITWG webinars.

A prospective EDE Entity will be responsible for sharing materials on CMS zONE with its Auditor(s) and any prospective upstream EDE Entities using its environment. CMS will provide updates with further requirements and resources as they become available. A prospective EDE Entity should regularly check the EDE 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 EDE.

D. REGTAP

CMS will make the trainings and a list of essential EDE resources available via REGTAP.[24]

E. Additional Guidance

- *Frequently Asked Questions Regarding Participation Requirements for Enhanced Direct Enrollment (EDE) Entities Serving Consumers in States with Federally-facilitated Exchanges (FFEs)*: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/FAQ-EDE-CY2019.pdf

[23] EDE documents and materials will be posted at the following link on CMS zONE: https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials.

[24] REGTAP can be accessed at the following link: https://www.regtap.info/.

- *Federally-facilitated Exchange (FFE) and Federally-facilitated Small Business Health Options Program (FF-SHOP) Enrollment Manual*: https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Enrollment-Manual-062618.pdf
- Web-broker Guidance on CMS 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
- For a current list of states that run their own State-based Exchange and do not use the federal platform, visit https://www.healthcare.gov/marketplace-in-your-state/. EDE Entities can use this list with state website links to refer consumers or agents/brokers in these states to their state’s website.
  - **Note:** Some states listed use the federal platform (HealthCare.gov) for individual coverage but run their own SHOP coverage operations. CMS will provide information to EDE Entities if changes are made in the future.