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

Date: **February 21, 2018**

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. Background

Beginning with the Open Enrollment Period (OEP) for plan year (PY) 2019, the Centers for Medicare & Medicaid Services (CMS) is implementing an optional program to allow Direct Enrollment (DE) entities[1] (qualified health plan [QHP] issuers and web-brokers[2]) in the Federally-facilitated Exchange (FFE, also referred to as Marketplace) and State-based Exchanges on the Federal Platform (SBE-FPs) to integrate an application for Marketplace coverage through the FFE with the standalone eligibility service (SES) to host application and enrollment services on their own website. The SES is a suite of application program interfaces (APIs) that will allow partners to create, update, submit, and ultimately retrieve eligibility results for an application. The Enhanced Direct Enrollment (EDE) pathway will replace the proxy DE pathway that CMS allowed DE entities to use for PY 2018. CMS will not allow DE entities' use of, nor will it support, the proxy DE pathway for PY 2019 and beyond.

When using the EDE pathway, a DE entity will provide a full application, enrollment, and post-enrollment support experience on its website, and must implement the full EDE application programming interface (API) suite of services, which includes Marketplace consumer records (MCR) for data matching issue (DMI) and special enrollment period (SEP) verification issue (SVI) status, as well as document storage and retrieval service (DSRS) for document upload and notice retrieval, and account creation ID proofing support. The DE 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. DE entities and CMS will accomplish this improvement by providing consumers in FFE and SBE FP states with more methods to shop and apply for Exchange coverage and by allowing consumers to work with a DE entity to enroll in a QHP without requiring consumers to log on to HealthCare.gov. The EDE

[1] References to "DE 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).

approach will provide a DE 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 approach will result in increased effectuation rates.

These guidelines discuss requirements and considerations for DE entities' selection of an auditor, program requirements, and the scope of the operational readiness review (ORR) DE entities must undertake to demonstrate they are prepared to provide DE services through use of the EDE pathway.

The ORR is governed by the CMS Expedited Lifecycle (XLC) process. For PY 2019, a DE entity that wishes to participate in EDE will submit an ORR composed of two separate audit packages: a business requirements audit and a privacy and security audit. Each DE entity must engage an independent auditor to perform the audits and certify that the entity's website(s) and operations comply with the program requirements listed in Table 2 and Table 3 of this guidance prior to CMS approving the DE entity to use the EDE pathway.

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

CMS will conduct ongoing oversight of each DE 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 Agreement, CMS requires each DE Entity using EDE to maintain a testing environment that accurately represents its production environment and 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, 156.265(b), and 156.1230, a DE 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 DE 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 DE entity must retain an independent third-party auditor to validate compliance with program requirements (see Section IV for guidance pertaining to the selection of an auditor). The DE 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 Agreement, which sets forth consumer communication and operational requirements, and an Interconnection Security Agreement (ISA), which sets forth privacy and security requirements. If an entity allows other DE entities to access its approved EDE pathway, CMS will permit the auditor(s) hired by the entity providing the EDE pathway to conduct the audit of the pathway for both the entity providing the pathway and for the entities accessing the pathway.

CMS will consider auditors to be downstream and delegated entities of a DE 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 DE entity will be responsible for auditor performance and for compliance with applicable program requirements.

II. Enhanced Direct Enrollment Business Requirements

A. Application Phase Options

CMS is offering DE entities three phases for hosting applications using the EDE pathway. In addition to hosting an application, a DE entity will need to integrate with the full EDE API suite. A DE entity may choose to implement Phase 1, 2, or 3 for the PY 2019 OEP (described below). The DE entity must commit to a phase prior to initiating its application audit because the ORR audit must reflect the compliance of the DE entity's operational EDE pathway. After conducting the audit for the upcoming OEP, the DE entity must not change phases without consulting CMS.

If a DE entity decides to switch to a different phase after its auditor has completed the business requirements audit, the auditor must re-conduct portions of the business requirements audit to account for any changes in the EDE pathway necessary to implement the newly selected phase. If the DE entity switches to a different phase after CMS has completed its review of the DE entity's business requirements audit for the phase the DE entity initially selected, CMS will review portions of the business audit requirements package for the newly selected phase as CMS resources allow. In such a scenario, CMS does not anticipate the auditor would need to re-conduct the DE entity's privacy and security audit.

A DE entity that implements Phases 1 or 2 is required to implement screening questions to redirect consumers whose circumstances it is unable to support to other supported application and enrollment channels. A DE entity will be required to support consumer-reported Changes in Circumstances (CiCs) and SEPs during and outside of the OEP, as well as supporting re-enrollment application activities. Table 1 describes each of the three end-state phases and explains their benefits.

Table 1. Application End State Phases

End State Phases	Description	Benefits
Phase 1: Host Simplified Application (App 2.0) + EDE API Suite	The DE entity hosts an application that cannot support all application scenarios, but will support only a subset of application scenarios equivalent to the current streamlined application user interface (App 2.0) implementation.	The DE entity could leverage the application created for proxy DE (if applicable) to reduce the amount of UI implementation required.

End State Phases	Description	Benefits
Phase 2: Host Expanded Simplified Application (App 2.0+) + EDE API Suite	The DE entity hosts an application that cannot support all application scenarios. The scenarios supported include the following: ▪ All scenarios covered by App 2.0 ▪ Full-time student ▪ Pregnant application members ▪ Non-U.S. citizens ▪ Naturalized U.S. citizens ▪ Application members who do not provide a Social Security Number (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	The DE entity could leverage the application created for proxy DE (if applicable) to reduce the amount of UI implementation required. EDE development would be streamlined, since not all application questions would be in scope.
Phase 3: Host Complete Application + EDE API Suite	The DE entity hosts an application that supports all application scenarios (equivalent to existing Classic application/App 3.0): ▪ All scenarios covered in Phase 2 ▪ American Indian and Alaskan Native application members	The DE entity would provide and service the full span of consumer scenarios. Additionally, the entity would no longer be required to support integration with the standard DE security assertion markup language (SAML) double redirect process.

In addition to the Application UI, DE entities are required to provide account management functions for consumers and conduct communications about their application and coverage status. These communications include, but are not limited to, providing statuses 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. Additional requirements for communications will be released at a later date.

B. 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 at the following link: https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials.

i. Business Requirements Audit Resources

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 DE entity's compliance with all business requirements, including those that the auditor has reviewed using CMS-provided toolkits.
- *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 Table 2. Each toolkit will provide testing scenarios that the auditor will use to verify the DE 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

DE entity's compliance. The DE entity must submit the completed templates to CMS as part of the business requirements audit package. CMS anticipates it will provide toolkits for Eligibility Results Testing, API Functional Integration Testing, Application Audit, UI Validation, and Consumer Communications requirements.

- *Phase-specific Requirements*: Some of the toolkits will include unique requirements, depending on the application phase that the DE entity has chosen to implement. For example, the Application Audit toolkit will encompass three separate toolkits, one for each of the three application phases (Phase 1, Phase 2, and Phase 3). Each toolkit will contain detail on specific questions that auditors must ask and any allowable flexibilities in question wording, question order, and question answer options for that specific phase. The auditor will use the phase-specific toolkit that corresponds with the application phase the DE entity has selected to implement to review the application UI on the DE entity's website and to assess the DE entity's compliance with the EDE application requirements. The auditor will use the Application Audit toolkit to verify the DE entity's compliance with Application UI requirements. CMS will provide additional information on the other toolkits as it becomes available.

ii. Privacy and Security Audit Resources

- *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 DE entity will use the SSP Workbook to create a final SSP, which will include detailed information about the DE entity's implementation of security and privacy controls. The auditor will review the SSP Workbook and final SSP to inform its assessment of the DE entity's compliance with the required privacy and security controls.
- *Security Privacy Assessment Test Plan (SAP) Template*: The SAP will contain a high-level description of the critical items that the auditor must test. The auditor should review this document prior to conducting the privacy and security audit.
- *Security Privacy Assessment Report (SAR) Template*: The auditor will be required to use this template to create a SAR. The SAR will verify that the DE entity has implemented the required privacy and security controls correctly.

C. Business Audit Scope

An auditor will complete a business requirements audit to ensure the DE entity has complied with applicable requirements as defined in this guidance. A DE 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 Table 2, which summarizes the review areas and review standards for the business requirements.

Table 2. Business Requirements

Review Category	Requirement and Audit Standard
Identity Proofing Implementation	▪ *Requirement*: The DE entity must conduct identity proofing for consumers entering the EDE pathway for enrollments through both consumer and agent/broker pathways. The DE entity must conduct identity proofing prior to submitting a consumer's application to the FFE. If the DE entity is unable to complete identity proofing of the consumer, the DE entity must either route the consumer to the traditional DE double-redirect pathway or direct the 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. The DE entity does not need to use third-party identity proofing if it already uses the approved FFE RIDP service. If the DE 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 the DE 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 the DE 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 Agreement. Applicants do not need to be ID proofed on subsequent interactions with the DE entity if the applicant creates an account (i.e., username and password) on the DE entity site. ▪ *Review Standard*: If the DE entity uses the FFE RIDP service, the auditor must verify the DE entity has successfully passed testing with the Hub. If the DE entity uses a third-party identity proofing service, the auditor must evaluate and certify that the identity proofing service is FICAM TFS-approved and that the DE entity has implemented the service correctly.
Phase-dependent Screener Questions (EDE Phase 1 and 2 DE entities Only)	▪ *Requirement:* A DE entity that implements either EDE Phase 1 or Phase 2 must implement screening questions to identify consumers whose eligibility circumstances the DE entity is unable to support consistent with the eligibility scenarios supported by the DE 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 are won't be able to apply through the EDE phase the DE entity implements, the DE 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 that the DE entity has implemented screening questions consistent with CMS guidelines to identify consumers with eligibility scenarios not supported by the DE entity's EDE pathway. CMS will release these screening questions at a later date. The auditor must verify that the entity's EDE pathway facilitates moving consumers to one of the alternative enrollment pathways described immediately above.

Review Category	Requirement and Audit Standard
Accurate and Streamlined Eligibility Application UI	▪ *Requirement*: DE entities participating in the EDE pathway must support all application scenarios outlined in the DE entity's selected phase. The DE entity must adhere to the guidelines set forth in the FFE Application UI Principles document when implementing the application. DE 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, the DE entity must implement the application in accordance with the FFE requirements. For each applicable eligibility scenario, the DE 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 DE entities to implement.) CMS will define appropriate flexibility DE 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., advance payments of the premium tax credit [APTC] attestation) must be identical to those of the FFE. – DE entities will also need to plan their application's back-end data structure to ensure that attestations can be successfully submitted to SES APIs at appropriate intervals within the application process and that the DE entity can process responses from SES and integrate them into the UI question flow logic, which is dynamic for an individual consumer based on their responses. The DE 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 document that the FFE Application UI has been implemented on the DE entity's pathway in accordance with the FFE Application UI Principles document and complies with the above standards. – The auditor will review the application for each supported eligibility scenario to confirm that the application has been implemented in accordance with the FFE Application UI Principles document. The auditor will document this compliance in the Application Audit Toolkit, embedded in the Application UI Companion Guide. – If the DE entity has implemented Phase 1 or Phase 2, the auditor will confirm that the UI includes a disclaimer stating that the pathway 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). Additional guidelines for this information will be released at a later date along with consumer communication information.

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, DMIs, SVIs, SEPs, and enrollment steps in a clear, comprehensive and consumer-friendly way. – The DE entity must provide consumers with the CMS-provided EDNs generated by the FFE any time it submits or updates an application pursuant to requirements provided by CMS in subsequent guidance. CMS will release the guidance at a later date. – The DE 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 will be set forth in the Consumer Communications toolkit. – The DE entity must provide and communicate ongoing statuses and access to information for consumers to manage their application and coverage. These communications include, but are not limited to, statuses 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. Additional clarification on these requirements will be released at a later date. ▪ *Review Standard*: The auditor must verify that the DE entity's EDE pathway notifies consumers of their eligibility results prior to QHP submission, including when submitting a CiC on the pathway. For example, if a consumer's APTC or cost-sharing reduction (CSR) eligibility changes, the DE 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. – The DE entity must have a process for providing consumers with a downloadable EDN in the EDE pathway and for providing access to a current EDN via the API. The DE entity must share required eligibility information that will be specified by CMS in subsequent guidance. – The auditor must verify that the DE entity's EDE pathway is providing statuses and ongoing communications to consumers according to CMS requirements 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:* The DE entity must provide consumers with CMS-provided language informing and educating the consumer about the Exchanges and HealthCare.gov and Marketplace-branded communications a consumer may receive with important action items. CMS will define these requirements in guidance. ▪ *Review Standard:* The auditor must verify that the DE entity's EDE pathway includes all required language, content, and disclaimers provided by CMS in accordance with the requirements stated in guidance. CMS will release this guidance at a later date.
Documentation of Interactions with Consumer Applications or the Exchange	▪ *Requirement:* The DE entity must implement tracking metrics on its EDE pathway 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 the DE entity's process for determining and tracking when an agent, broker, and consumer has interacted with a consumer application or actions utilizing the EDE pathway.

Review Category	Requirement and Audit Standard
Eligibility Results Testing and SES Testing	▪ *Requirement*: The DE entity must submit accurate applications through the EDE pathway that result in accurate and consistent eligibility determinations for the consumer eligibility scenarios covered by the DE entity's chosen EDE phase. – The business requirements audit package must include testing results, either in the existing FFE test environment or the final implementation of the EDE pathway, depending on the timing of the submission. CMS will provide a resource on CMS zONE containing the eligibility scenarios for auditors to test on the EDE pathway or FFE testing environment. ▪ *Review Standard*: The auditor must complete a series of test eligibility scenarios using the DE entity's EDE pathway implementation. For example, these scenarios may include Medicaid and Children's Health Insurance Program (CHIP) eligibility, and different combinations of APTC and CSRs. 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, with expected eligibility results received, and to submit FFE Application IDs and EDNs, when applicable, for each test scenario.
API Functional Integration Requirements	▪ *Requirement*: The DE entity must implement the EDE API suite in accordance with the API specifications provided by CMS. CMS will release these specifications questions at a later date. ▪ *Review Standard:* The auditor must complete a set of consumer testing scenarios to confirm that the DE entity's API integration performs the appropriate functions when completing the application. 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. The functional integration testing scenarios will be available in the API Functional Integration Testing toolkit.
Application UI Validation	▪ *Requirement:* The DE entity must implement CMS-defined validation requirements within the application. The validation requirements prevent the DE entity from submitting incorrect data to the FFE. ▪ *Review Standard:* The auditor must confirm that the DE entity's application has implemented the appropriate field-level validation requirements consistent with CMS requirements. These field-level validation requirements will be documented in the FFE Application UI Principles.
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. § 155.265(d)(3)(iii) (citing 45 C.F.R. §§ 155.230 and 155.260), the DE entity 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 the DE 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)).

D. Third-party Agent and Broker Arrangements

A DE entity must perform data collection only through its approved EDE pathway, and cannot collect consumer eligibility application information for the EDE pathway on any website or application other than approved websites identified in the DE entity's EDE pathway application process submitted to CMS. These websites will be subject to oversight by CMS. Any implementation of a DE entity's EDE pathway must be consistent with the audit report approved by CMS.

A DE entity may allow third-party agents and brokers who are registered with the FFE to use its respective approved EDE pathway to assist consumers in supported states with applying for coverage, as well as APTC and CSRs, and with selecting QHPs. However, the DE entity must not provide the capability for third-party agents or brokers or other downstream and delegated entities who are not or will not be a party to their own EDE Agreement with CMS to use its EDE

pathway on the third-party's own website or otherwise outside of the DE entity's approved website and EDE pathway.

Additionally, a DE entity is responsible for ensuring compliance with the terms and conditions of the EDE Agreement by all downstream third-party agents and brokers who access and use its approved EDE pathway.

E. Entities Providing an EDE Pathway

CMS will permit an entity to develop and provide its approved EDE pathway to one or more DE entities. The entity providing the pathway should develop the two parts of the ORR (the business requirements audit and the privacy and security audit) that will produce the applicable audit findings for all DE entities using the identical version of the entity's approved EDE pathway.

In this scenario, CMS will permit minor deviations for branding on the approved EDE pathway. The entity developing the pathway and any upstream DE entities using that pathway (e.g., QHP issuers) must both submit an EDE Agreement and identify the arrangement within the EDE Agreement. The upstream entity will be responsible for complying with all requirements in regulation, applicable guidance, and the EDE Agreement, including oversight of the entity providing the EDE pathway.

If a DE entity will use another entity's approved EDE pathway, while adding additional functionality or systems to complete the implementation of its own EDE pathway (e.g., the approved EDE pathway of the other DE entity does not comprise the entire EDE pathway for a DE entity), the DE entity will need to conduct and resubmit the applicable part of the ORR with additional findings for any added functionality or systems to confirm the DE entity's compliance with applicable CMS regulations and the EDE Agreement, as appropriate.

If a DE entity is using an approved EDE pathway and the associated ORR audit packages provided by another entity, the DE entity must indicate in its EDE Agreement and in its ISA that it is using an approved EDE pathway provided by another entity and be prepared to submit a copy of the business requirements audit package, privacy and security audit package, and documentation of the arrangement upon request by CMS.

If a DE entity will use an approved EDE pathway provided by another entity, but such pathway will not comprise the totality of the DE entity's implementation of its own EDE pathway (consistent with the example above), the DE entity must submit two ORR audit packages that contain both the results of the audits for the EDE pathway provided by the other entity, as well as the results of the ORR that cover any additional systems or requirements that complete the DE entity's EDE pathway.

III. Privacy and Security Requirements

An auditor will complete a privacy and security audit to ensure that the DE entity complies with applicable requirements as defined in CMS regulations and this guidance. A DE entity must submit the resulting privacy and security audit package to CMS. Table 3 describes the review areas and review standards for the privacy and security requirements.

Table 3. Privacy and Security Requirements

Review Category	Audit Standards
Privacy and Security Control Implementation	▪ *Requirement:* A DE entity must implement security and privacy controls, 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 DE entity as defined by CMS in the ISA. ▪ *Review Standard*: The auditor must conduct a Security and Privacy Control Assessment (SCA) and produce a SAR to certify that the DE entity has implemented processes sufficient to meet the privacy and security requirements set forth in the ISA and in applicable regulations. – If the auditor determines that the DE entity does not meet one or more privacy and security requirements, the DE 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 DE entity will come into compliance with each requirement and will state the estimated completion date for each identified milestone. Auditors must verify that the DE 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.

IV. Selection of an Auditor

A DE 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 DE entity's engagement of its auditor(s) and the auditor(s)' work in relation to the engagement. Each DE entity must identify its selected auditor(s) in the EDE Agreement and the ISA between CMS and the DE entity.

A. Allowance for Multiple Auditors

A DE entity is permitted to select either one auditor to complete both the business requirements audit and the privacy and security audit or the entity may select two auditors, one to complete the business requirements audit and the other to complete the privacy and security audit. If the DE 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 DE entity retains two auditors to complete the audits, it should notify CMS of this arrangement and provide the contact information for both auditors, including designating 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 DE entity.

B. Required Experience

HHS will require that a DE entity selects auditor(s) with the experience outlined below and attest, within the EDE Agreement and the ISA, that the auditor(s) have demonstrated or possess such experience.

i. Business Requirements Auditor Experience

CMS will require that the auditor selected by DE 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 DE entity can 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. Privacy and Security Auditor Experience

CMS will require that the key personnel of an auditor selected by a DE 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; 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 DE 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.

C. Recommended Experience

i. 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. A general familiarity and understanding of reading Simple Object Access Protocol (SOAP) XML responses from the FFE APIs will 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 DE entity's pathway and if the DE entity provides information relevant to the audit in a user-friendly interface or in raw XML file format. CMS anticipates providing limited training and technical assistance to DE entities and auditors on understanding and reading the DE XML files.

ii. Privacy and Security Auditor Experience

CMS strongly recommends that an auditor selected to conduct the privacy and security audit have prior FISMA experience. Prior FISMA experience will aid an auditor in assessing a DE

entity's compliance with the required privacy and security controls, and producing a high-quality SAR.

D. Conflict of Interest

A DE 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 DE 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).

V. Required Auditor and DE entity Training

The auditor(s) selected by the DE entity and representative(s) from the DE entity are required to take CMS-mandated training. 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.

- 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 potentially other 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, EDE ORR and CMS Reporting Requirements, and other potential modules to be defined by CMS. Representative(s) from the DE entity must take all training modules.

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 March 2018. All training modules will be posted on REGTAP as they become available.

VI. Required Documentation

Table 4 includes the documentation, and any associated templates, a DE entity must submit to be approved to use the EDE pathway and for planning and completing the two audit packages pursuant to CMS requirements. CMS will provide additional information regarding reporting and document submission.

Table 4. Required Documentation

Document	Description	Submission Requirements
Notice of Intent to Participate	▪ A QHP issuer or web-broker must notify CMS if it intends to apply to use the EDE pathway for PY 2019, beginning with the PY 2019 OEP. CMS will follow up with a request for additional information.	▪ The QHP issuer or web-broker should email directenrollment@cms.hhs.gov ▪ Subject line should state: "Enhanced DE: Intent."

Document	Description	Submission Requirements
EDE Business Agreement	▪ A DE entity must submit the EDE Agreement to use the EDE pathway. The agreement must identify the DE entity's selected auditor. ▪ CMS will countersign the EDE Agreement after CMS has reviewed and approved the business requirements audit and the privacy and security audit findings reports.	▪ A DE entity should submit the EDE Agreement via the secure portal.
Auditor Resources Package	▪ A DE entity must submit the Business Requirements Audit Report Template, Application Audit Template, and other applicable templates completed by its auditor.	▪ A DE entity should submit the different parts of the auditor resources package via the secure portal.
Interconnection Security Agreement (ISA)	▪ A DE 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 findings reports.	▪ A DE entity should submit the ISA via the secure portal.
Security Privacy Assessment Report (SAR)	▪ This report details the auditor's assessment of the DE entity's security and privacy controls implementation.	▪ A DE entity should submit the SAR completed by its auditor via the secure portal.
Plan of Actions & Milestones (POA&M)	▪ A DE 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 DE entity should submit the POA&M in conjunction with the SAR via the secure portal.
Privacy Impact Assessment (PIA)	▪ The PIA will detail the DE entity's evaluation of its controls for protecting PII.	▪ A DE entity is not required to submit the PIA to CMS. However, per the ISA, CMS may request and review the DE entity's PIA at any time, including for audit purposes.
System Security and Privacy Plan (SSP)	▪ The SSP will include detailed information about the DE entity's security and privacy controls.	▪ A DE entity is not required to submit the SSP to CMS. However, per the ISA, CMS may request and review the DE entity's SSP at any time, including for audit purposes.
Incident Response Plan and Incident/Breach Notification Plan	▪ A DE entity is required to implement breach and incident handling procedures that are consistent with CMS' Incident and Breach Notification Procedures. ▪ A DE entity must incorporate these procedures into its own written policies and procedures.[3]	▪ A DE 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 the DE entity's Incident Response Plan and Incident/Breach Notification Plan at any time, including for audit purposes.

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

Document	Description	Submission Requirements
Contingency Plan	▪ A DE entity is required to complete a Contingency Plan that describes the backup plan that the DE entity will implement if the DE entity's system(s) are down.	▪ A DE entity is not required to submit this the Contingency Plan to CMS. However, per the ISA, CMS may request and review the DE entity's Contingency Plan at any time, including for audit purposes.

VII. Secure Portal for Document Submission

CMS will require a DE entity applying to participate in EDE to submit documents to CMS via a secure portal. After the DE entity informs CMS that it has entered into an agreement with its auditor(s), CMS will assign the DE entity a unique identification code that the DE 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 DE entities to encrypt documents containing proprietary information before uploading them to the portal.

VIII. Approval Process

A. Application UI Feedback Process

Prior to publicly launching an EDE application, a DE entity can request feedback from CMS on its planned application UI build. A DE entity and/or its auditor can submit a request for application UI feedback from CMS through the secure portal. The purpose of this process is to answer clarification questions about application requirements and mitigate the risk that CMS identifies compliance issues during the CMS-conducted mini audit (discussed in Section VIII.B 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 DE entity and/or auditor 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 DE entity may submit application UI feedback requests up until the completion of the business requirements audit; upon submission of the audit, the DE entity's application should be finalized. If CMS determines a discussion with the DE entity and/or auditor is needed, CMS will schedule a meeting between the DE entity and/or auditor, the DE entity's 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 DE entities on the application and UI, the auditor will verify compliance with guidelines and requirements.

B. Enhanced DE Oversight

When CMS receives a final business requirements audit package that confirms a DE entity's application UI complies with application guidelines and requirements, CMS will conduct a mini audit of the DE entity's application prior to final approval of the EDE pathway. The DE entity will be required to provide CMS, via the DE Help Desk, with a set of credentials that CMS can use to access the testing environment to complete the mini audit of the EDE pathway. The DE entity must ensure that the testing credentials are valid and that all APIs and components of the

EDE pathway in the testing environment, including the RIDP services, are accessible for the duration of the mini audit.

CMS will review any compliance issues identified during the mini audit and provide written feedback to the DE entity of changes that the DE entity will be required to make prior to final approval. The DE 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 DE entity's EDE pathway 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 mini audit, CMS will require the DE 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 post-production changes in a DE entity's EDE pathway.

C. Final Approval Process

CMS will review and approve DE entities to use the EDE pathway on a first-come, first-served basis. CMS recommends that each DE entity select its auditor(s) and submit its documentation by August 15, 2018, or as soon as is feasible without jeopardizing the integrity of the ORR process or the FFE eligibility determination process and implementation.

CMS will notify DE entities on a rolling basis of approval to use the EDE pathway. CMS will countersign a DE entity's EDE Agreement and ISA after CMS reviews and approves the DE entity's business audit package and privacy and security audit package, and after it confirms that the DE entity's EDE pathway is functional in the final technical implementation in the FFE testing environment. After CMS countersigns the EDE Agreement and the ISA, CMS will inform the DE entity of the subsequent steps to implement the EDE pathway.

IX. Resources

A. Help Desk

In addition to hosting weekly webinars inclusive of interactive question and answers, CMS currently manages multi-team DE entity-facing help desks to address questions, technical problems, operational issues, other issues, and policy questions for all DE entities. A DE entity must either remove PII in documents before sending them to the help desks or encrypt the e-mail transmitting the PII.

A DE 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]." A DE entity may also use the FEPS Help Desk to send technical questions asked by its auditor(s).

A DE entity with technical questions specifically related to Hub onboarding for DE in general, Hub onboarding for the various DE/EDE APIs, connectivity issues related to accessing the DE 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 DE team.

For a timely response, the DE 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 HIOS ID (if an existing issuer) or DE entity 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. This summarization 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 DE, please include the request/response XMLs/JSONs for troubleshooting (API requests and responses). DE entities must remove PII prior to sending the XML/JSON to the FEPS Help Desk or Hub Help Desk, or the DE entity must encrypt the email.

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

A DE 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 following section for webinar details.

If a DE 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. Potential Webinars

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. The call-in information is as follows:

Dial-in: 1-877-267-1577
ID: 2284-2124
Webinar URL: https://webinar.cms.hhs.gov/issuertechnicalworkgroup/

CMS will continue to use the ITWG call to update the DE community on developments related to EDE and offer interactive question and answer time at the end of each session.

CMS anticipates hosting a separate, additional webinar forum focused solely on those specific issuers and web-brokers interested in implementing EDE, leading up to the start of the 2019

OEP. These webinars will include interactive questions and answer sessions to focus on EDE specific topics, such as questions about EDE testing best practices. CMS encourages DE entities to bring their auditors to these sessions.

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 at the following link: https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials. This webpage is accessible by members of the Private Issuer Community (for issuers) and the 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 technical webinars.

A DE entity will be responsible for sharing materials on CMS zONE with its auditor(s) and any upstream DE entities using its pathway. CMS will provide updates with further requirements and resources as they become available. A DE 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 FAQs available via REGTAP. CMS may also make other limited information pertaining to the EDE pathways, business requirements audit and privacy and security audit available on REGTAP.

E. Additional Guidance

- *Federally-facilitated Marketplace (FFM) and Federally-facilitated Small Business Health Options Program (FF-SHOP) Enrollment Manual*: https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/ENR_FFMSHOP_Manual_080916.pdf
- Web-broker Guidance on CMS Agents/Brokers Resources 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/. DE entities can use this list with state website links to refer consumers or agents/brokers in these states to their state's website. Note, some states listed use the federal platform (HealthCare.gov) for individual coverage but run their own SHOP coverage operations. CMS will provide information to DE entities if changes are made in the future.