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

Overview of Enhanced Direct Enrollment (EDE) Oversight

February 22, 2019

Intended Audience and Purpose

- The intended audience for this presentation is web-brokers, agents, brokers, issuers offering Qualified Health Plans (QHPs), technology providers, potential Auditors, and others who are interested in learning about the EDE program at CMS.
- The purpose of this presentation is to provide a high-level overview of the EDE program, EDE oversight, program timelines, and other important considerations for those interested in seeking approval to participate.
- CMS released the detailed set of guidelines on February 19, 2019: https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Guidelines-for-Third-party-Auditors-EDE-PY19PY20.pdf
  - EDE Entities already approved to use the EDE pathway or prospective EDE Entities awaiting approval for EDE will need to review the detailed set of updated guidelines.

Agenda

- EDE Introduction
- EDE Oversight Requirements
- Business Requirements Audit
- Security and Privacy Audit
- Questions

Topics To Be Covered

- Topics covered in this webinar include:
  - Application Phase Options
  - Resources for Current and Prospective EDE Entities
  - Options for Participating
  - EDE Development and Timeline Considerations
  - EDE Approval Process Timeline
  - Audit Submission Considerations
  - Information Security and Privacy Continuous Monitoring

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF TECHNOLOGY SOLUTIONS

EDE Introduction

EDE Background

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

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

EDE End State Scope Options

- CMS is offering prospective EDE Entities three phases for hosting applications using the EDE pathway. A prospective EDE Entity may choose to implement Phase 1, 2, or 3 for PY 2019 and PY 2020.

End State Scope Option	Description	Benefit
Phase 1: Host Simplified Application + EDE API Suite	The EDE Entity hosts an application but chooses to support a subset of 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.

EDE End State Scope Options (Continued)

- CMS is offering prospective EDE Entities three phases for hosting applications using the EDE pathway. A prospective EDE Entity may choose to implement Phase 1, 2, or 3 for PY 2019 and PY 2020.

End State Scope Option	Description	Benefit
Phase 2: Host Expanded Simplified Application + EDE API Suite	The EDE Entity hosts an application but cannot support all application scenarios. The supported scenarios would include: • All scenarios covered by Phase 1 • Full-time students • 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 card • 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.
Phase 3: Host Complete Application + EDE API Suite	The EDE Entity hosts an application that supports all scenarios (equivalent to HealthCare.gov).	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.

EDE End State Scope Options (Continued)

- What are the additional scenarios required to go from Phase 2 to Phase 3 implementation?
  - Application members who live at different home addresses
  - Married couples filing separate tax returns
  - Application filers who do not file a tax return or who are claimed as tax dependents
  - Adult applicants responsible for children aged 18 or younger whom they do not claim on their tax return
  - Application members who are eligible for health coverage through a job or COBRA
  - Application members who have tax dependents who are not their sons/daughters
  - Child age applicants who live with a parent who is not part of their tax household

EDE APIs

- EDE Entities integrate their systems with CMS' systems through software-to-software information exchange interfaces, which are known as APIs.

Class of API	Functionality	Example APIs
Eligibility APIs	• Enable EDE Entities to create, update, delete, submit, or view a consumer's application.	• Create App from Prior Year; Create App; Get App; Update App; Add Member; Remove Member; Submit App
Enrollment APIs	• Provide EDE Entities with the capabilities to retrieve enrollment/policy data in real time. • Allow EDE Entities to submit enrollments.	• Submit Enrollment
Customer Service/ Account Management APIs	• Check data-matching issue (DMI) and/or Special enrollment period (SEP) verification issue (SVI) status. • Store the ID proofing record and establish permission for EDE Entities to perform work on behalf of the consumer. • Upload documents for DMI/SVI adjudication. • Retrieve Exchange notices. • Complete payment redirect to issuer websites for eligible consumers.	• Get DMI; Get SVI; Notice Retrieval; Document Upload; Payment Redirect; Store ID Proofing Record

EDE APIs (Continued)

- **The EDE API Suite includes the following APIs:**
  - Create App
  - Create App from Prior Year App
  - Add Member
  - Remove Member
  - Update App
  - Submit App
  - Get App
  - System and State Reference Data
  - Person Search
  - Get Enrollment
  - Metadata Search
  - Notice Retrieval
  - Document Upload
  - Store ID Proofing
  - Get DMI
  - Get SVI
  - Store Permission
  - Submit Enrollment
  - Optional APIs:
    - Delete App
    - Payment Redirect
    - Fetch Eligibility (EDE Entities can opt to use a combination of Get App, Get Enrollment, and Get SVI to get the same information)
    - RIDP (if an EDE Entity has a consumer flow, they'll have to either use this, or a 3rd party FICAM TFS approved provider);
    - FARS
    - Event-Based Processing (Likely deploying to Production in May of 2019)

EDE Business Flow: Summary of Changes from Classic DE

- Consumer starts on the EDE Entity's website and stays on the EDE Entity's website the entire time (no double redirect).
- EDE Entity can customize the consumer eligibility application (within program flexibility requirements).
- Consumer can upload documentation to resolve SVIs and DMIs from the EDE Entity's website.
  - In Classic DE, consumer needs to complete an additional redirect to upload documentation.
- EDE Entity can easily offer payment redirect to the consumer.
  - In Classic DE, the burden is on the DE Entity to set up a payment redirect connection with each issuer they sell plans for, whereas in EDE the EDE Entity can simply integrate with the Payment Redirect API.
- Consumers can view their current policy status, along with the status of any outstanding SVIs or DMIs directly from the EDE Entity's website.
  - In Classic DE, consumers need to complete an additional redirect to view this information.
- Consumer can download notices from the EDE Entity's website.
  - In Classic DE, consumers need to complete an additional redirect to obtain notices.
- Consumer can always return to the EDE Entity's website for changes in circumstances (CiCs) and SEPs.
  - Some Classic DE Entities do not support CiCs and SEPs outside of OEP, but EDE Entities are required to support changes outside of the OEP.

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF TECHNOLOGY SOLUTIONS

EDE Oversight Requirements

EDE Oversight

- For more information on basic EDE program requirements and details, refer to the updated EDE guidelines that were released in February 2019: https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Guidelines-for-Third-party-Auditors-EDE-PY19PY20.pdf
- Prospective EDE Entities can begin developing their EDE environments based on the toolkits and security and privacy documentation that are located on CMS zONE.
- To pursue EDE, prospective EDE Entities must build their EDE environments and security programs. Then, prospective EDE Entities must have one or more third parties conduct audits consisting of two parts (a Business Requirements Audit and a Security and Privacy Audit). The audits must be submitted to CMS within the submission windows established by CMS.
- The primary audit submission window for prospective EDE Entities interested in implementing EDE in calendar year 2019 for PY 2019 and PY 2020 is April 1, 2019 to June 30, 2019.
- **Notice of Intent**: If a prospective EDE Entity intends to submit its audit during the April 1, 2019 to June 30, 2019 submission window, it must send its notice of intent to directenrollment@cms.hhs.gov by February 28, 2019.
  - CMS will release future guidance about the next annual audit submission window after the PY 2020 OEP.

EDE Resources on CMS zONE for Current DE Entities

- Prospective EDE Entities can begin developing their EDE environments based on the existing toolkits and security and privacy documentation that are located on CMS zONE.
  - Note that prospective EDE Entities must set up a CMS Enterprise Portal account and request zONE access to view the zONE website.
  - Prospective EDE Entities must share all EDE audit resources with their Auditors as CMS zONE site access is restricted to prospective and approved EDE Entities (participating web-brokers and issuers) and their representatives only.
  - CMS will not distribute this documentation through any other methods.

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

- Prospective EDE Entities that are not already DE Entities and cannot access CMS zONE may view several publicly available resources:

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

April 1 – June 30 EDE Audit Submission Window

- Assumptions for prospective EDE Entities intending to submit audits during the April 1, 2019 to June 30, 2019 submission window:
  - Prospective EDE Entities must submit complete audits between April 1, 2019 and June 30, 2019 to have a chance to be approved for EDE during calendar year 2019.
  - EDE Entities that are already live with EDE and intend to implement a new phase must also submit audits between April 1, 2019 and June 30, 2019.
  - If a prospective EDE Entity submits an audit and resubmits it before hearing from CMS about its original submission, CMS will only consider the date of the latest submission for purposes of determining review priority.
  - CMS will require that incomplete audits be resubmitted in their entirety and will prioritize review of these resubmitted audits based on the date the complete audit is submitted.
    - CMS will not accept resubmitted audits after June 30, 2019, but prospective EDE Entities may be required to resubmit components of audits that CMS previously determined were complete. This may occur when a complete audit does not represent a compliant implementation and deficiencies must be corrected and documented before approval.
  - 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.
  - Once the prospective EDE Entity resubmits a complete audit, CMS will consider that resubmitted audit to be at the end of the review queue based on the date of submission. CMS does not guarantee any approval timelines.

Options to Participate

- Prospective EDE Entities have two (2) main options to consider in determining how and to what extent to pursue participation in EDE during calendar year 2019:
  - Participate as a primary EDE Entity that has developed its own EDE environment and contracted with an Auditor to audit the environment, or
  - Participate as an upstream EDE Entity of an approved primary EDE Entity, which may not require an independent audit of the upstream entity's systems (i.e., primary EDE Entities may provide an EDE environment to another entity like an issuer or web-broker).

Options to Participate (Continued)

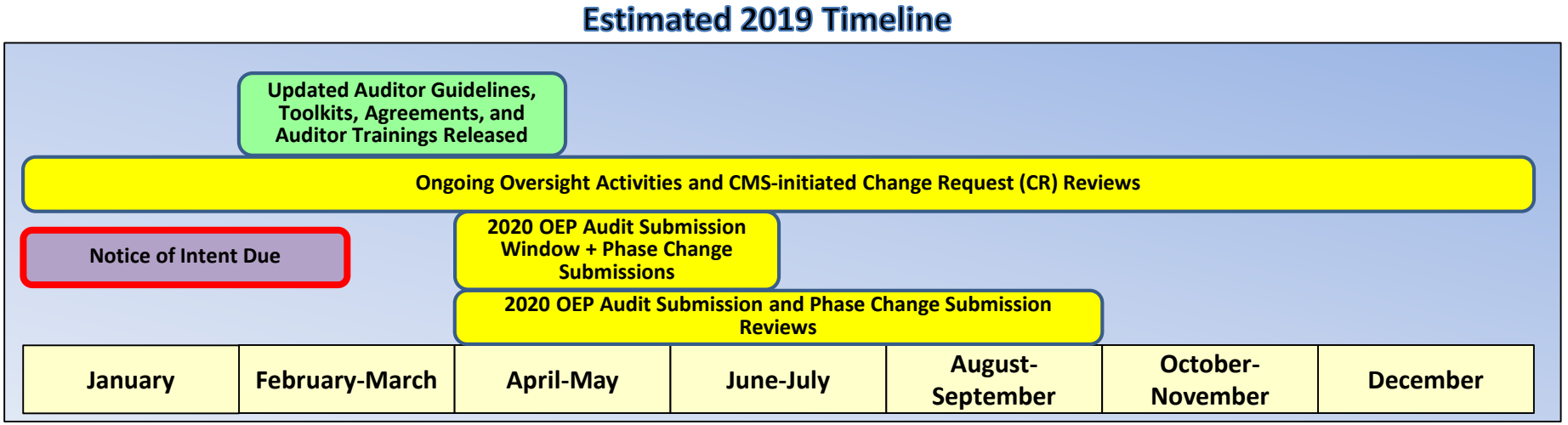
- Prospective EDE Entities that wish to participate in EDE independent of another entity must first be approved to participate in DE as an issuer or web-broker.
- Prospective upstream EDE Entities that are not already participating in DE (also known as "Classic DE" and "double redirect") as a web-broker or issuer may contract with either an issuer that has a QHP issuer agreement or a web-broker that has a web-broker agreement to develop or provide the prospective upstream EDE Entity with an EDE environment.
- All upstream EDE Entities must have a legal relationship with a primary EDE Entity. The primary EDE Entity will be a delegated or downstream entity of the upstream EDE Entity.
- The list of EDE Entities (both primary and upstream) that are approved to use the EDE pathway is available here.
  - This list is updated frequently, but it may not immediately reflect EDE Entities most recently approved to use the EDE pathway.

EDE Development and Timeline Considerations

- Developing and auditing an EDE environment takes considerable effort and time (it may take up to or more than a year).
- CMS strongly recommends prospective EDE Entities start developing their EDE environments as early as possible.
- CMS strongly recommends prospective EDE Entities integrate security and privacy safeguard measures into the design, development, and implementation of their EDE information system and continue these measures throughout maintenance, operation, and disposal within their organizationally defined system development life cycle (SDLC).
- CMS recommends that issuers and web-brokers have appropriately skilled staff before attempting to implement EDE. This staff should include programmers capable of building websites and integrating with APIs. Entities would also benefit from having staff that are familiar with Marketplace eligibility and enrollment policies, as well as security and privacy best practices.

CMS' review of the audit submission may take several months, depending on the quality of the EDE Entity's EDE environment and audit.

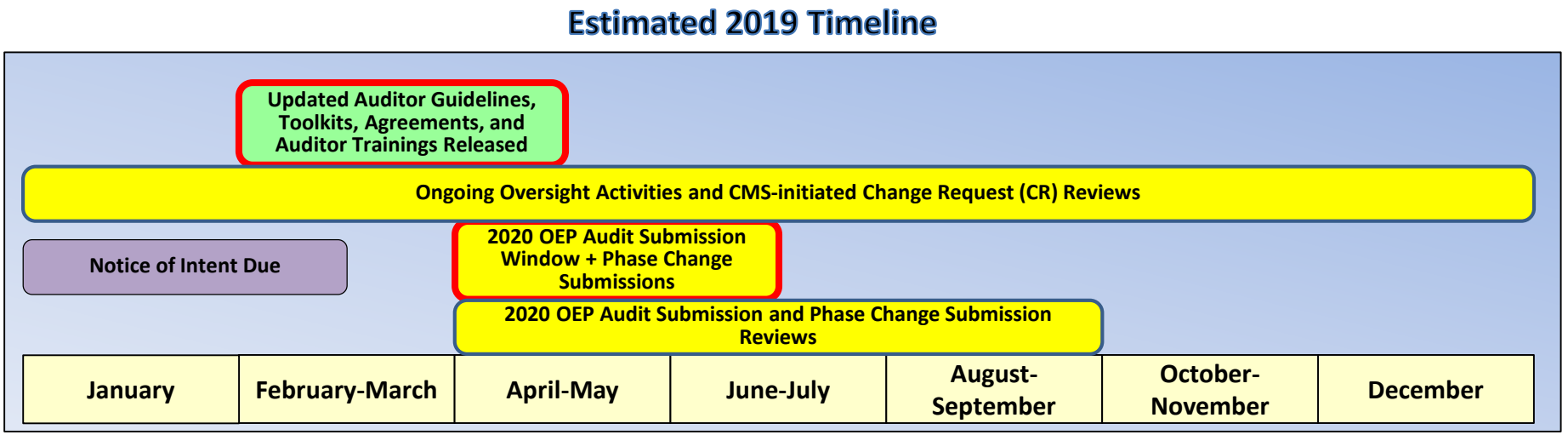
EDE Approval Process Timeline



- **Notice of Intent**: If a prospective EDE Entity intends to submit its audit during the April 1, 2019 to June 30, 2019 submission window, it must send its notice of intent to directenrollment@cms.hhs.gov by February 28, 2019.

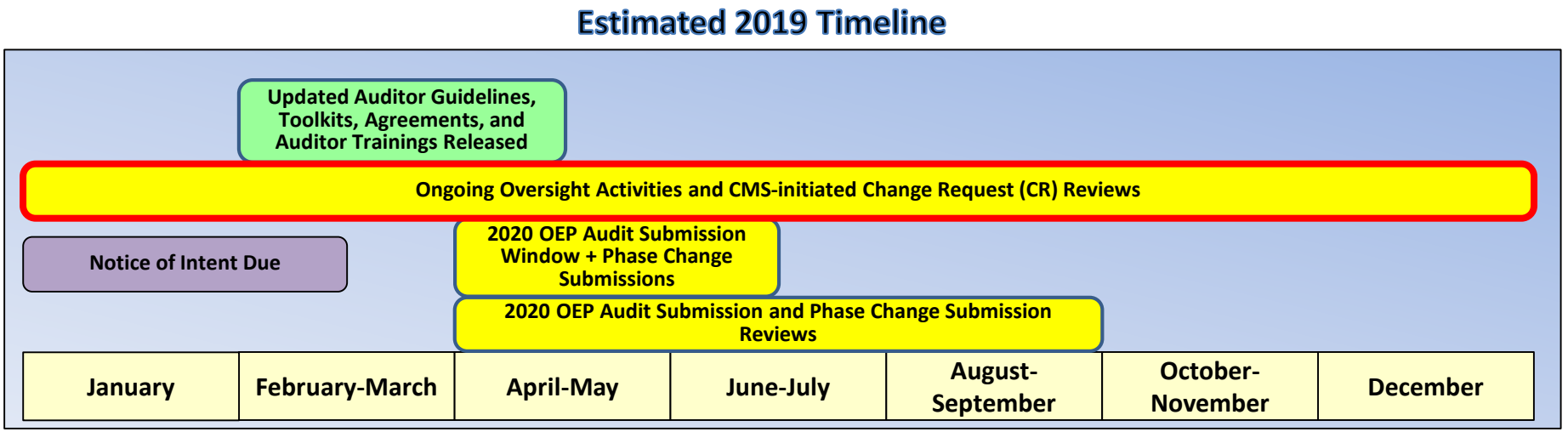
- The subject line of a notice of intent email must read "Enhanced DE: Intent" and the information below must be included in the body of the email:
  - Prospective EDE Entity Name;
  - Auditor Name(s) and Contact Information (Business Requirements and Security and Privacy, if different);
  - EDE Phase (1, 2, or 3);
  - Prospective EDE Entity Primary Point of Contact (POC) name, email, and phone number;
  - Prospective EDE Entity Technical POC name, email, and phone number;
  - Prospective EDE Entity Emergency POC name, email, and phone number; and
  - CMS-issued Hub Partner ID.

EDE Approval Process Timeline (Continued)



- 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 to June 30, 2019 submission window in early 2019. CMS expects to primarily use the same content and requirements as in the materials released in 2018 for PY 2019.
- Please refer to slide 29, "Baseline Versions of Business Report Template and Toolkits for Prospective EDE Entities Submitting Audits," for more information on baseline toolkits.
- There is no guarantee that every prospective EDE Entity that submits a complete audit in the submission window will receive approval unless and until the Entity meets all program requirements.
  - CMS offers no guarantee that every prospective EDE Entity that submits a complete audit submission by June 30, 2019 will receive approval to go live in PY 2019 or before/during the PY 2020 OEP because the content and quality of the audit submissions vary substantially and that affects the amount of time it takes to review.

EDE Approval Process Timeline (Continued)



- There may be more CMS-initiated Change Requests (CRs) as we get closer to the 2020 OEP. EDE Entities will be required to implement applicable CRs by the respective deadlines.
  - CMS-initiated CRs may occur year-round. CMS will conduct ongoing oversight activities throughout the PY 2020 OEP.
- CMS has previously issued information on CMS-initiated CRs in the FAQ titled "What is the CMS-Initiated Change Request Process for DE Entities Using EDE in Plan Year 2019?" in the EDE Compliance FAQs available at the following link: https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials. CMS strongly encourages prospective EDE Entities to review this FAQ.

Required Auditor and Prospective EDE Entity Training

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

If a 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).

Independence of the Auditor

- An independent third-party Auditor is independent if there is no perceived or actual conflict of interest involving the developmental, operational, and/or management chain associated with the system and the determination of effectiveness (e.g., security and privacy control effectiveness).
- The Auditor's role is to provide an independent assessment of the compliance of the EDE Entity's EDE environment and to maintain the integrity of the audit process.
- Within the Security and Privacy Controls Assessment Test Plan (SAP) which is submitted to CMS, the Auditor will be required to attest to his or her independence and objectivity in completing the audit, and that neither the EDE Entity nor the Auditor took any actions that might impair the objectivity of the findings in the audit.

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF TECHNOLOGY SOLUTIONS

Business Requirements Audit

Overview of Business Requirements Audit

- An Auditor will complete a business requirements audit to ensure the prospective EDE Entity has complied with applicable requirements as defined in CMS' EDE implementation guidance.
- The business requirements audit focuses on, but is not limited to, the following requirements:
  - Identity proofing of consumers and agents/brokers;
  - Eligibility application user interface (UI) (e.g., accuracy, correct implementation, and validation);
  - Communications (e.g., post-eligibility communications and accurate communications about the Exchange and consumer communications);
  - Documentation of interactions with consumer applications or the Exchange;
  - Eligibility results testing and Standalone Eligibility Service (SES) testing;
  - Functional integration of APIs;
  - Section 508 compliance; and
  - Non-English language versions of relevant audit components.

Audit Submission Considerations: Having a Complete Business Requirements Audit

- **Complete Audit:** A complete business requirements audit submission meets the following criteria, at a minimum:

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

Audit Submission Considerations: Having a Complete Business Requirements Audit (continued)

- **Incomplete Audit:** An incomplete business requirements audit does not meet the completeness criteria described above. The Auditor must complete incomplete audits in accordance with the standards described above. CMS will require that incomplete audits be resubmitted in their entirety and will prioritize its review of these resubmitted audits based on the date the complete audit is submitted.
  - Business requirements audits should not include comments that describe the Auditor's process for verifying the requirement unless there is a specific issue or concern regarding the requirement that warrants raising a concern.

Baseline Versions of Business Report Template and Toolkits for Prospective EDE Entities Submitting Audits

- CMS will establish a "baseline" version of the Business Requirements Audit Report Template and each accompanying toolkit in early 2019. CMS will release the toolkits on CMS zONE as they become available.
- Prospective EDE Entities can begin developing their EDE environments based on the existing toolkits and security and privacy documentation that are located on CMS zONE.
- ***Until the new baseline versions are available, CMS strongly encourages prospective EDE Entities and Auditors to use the latest version of each toolkit as indicated in the right-most column, as doing so will reduce the number of separate CMS-initiated CRs that prospective EDE Entities will need to implement.***
- An FAQ with further information is available within the **EDE Compliance FAQs** on CMS zONE here (see "Does CMS have any guidance for using the updated Business Requirements Audit Report Template and toolkits once we have begun the business requirements audit?"): https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials.

Business Toolkits/Templates

Toolkit & Template	Document Name	Most Recent Version
API Functional Integration Toolkit	API_Functional_Integration_Toolkit_PY2019_01192019.xlsx	Posted 1/19/2019
Communications Toolkit	Communications Toolkit_09062018.xlsx	9/6/2018
Application User Interface (UI) Toolkit	Application UI Toolkit_PY2019_02082019.xlsx	2/8/2019
Eligibility Results Toolkit(s) for PY 2019	EDE_Eligibility Results Toolkit_Phase 1_PY2019_FINAL.xlsx EDE_Eligibility Results Toolkit_Phase 2_PY2019_FINAL.xlsx EDE_Eligibility Results Toolkit_Phase 3_PY2018_FINAL.xlsx	2/6/2019
EDE Business Audit Instructions and Report Template	EDE Business Audit Instructions and Report Template_07052018.docx	7/5/2018

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF TECHNOLOGY SOLUTIONS

Security and Privacy Audit

Overview of Security and Privacy Audit

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

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

Auditor Experience

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

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

Submission Process Considerations: Having a Complete Security and Privacy Audit

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

Submission Process Considerations: Having a Complete Security and Privacy Audit

Document	Minimum Requirements for a Complete Audit
Security and Privacy Controls Assessment Test Plan (SAP)	▪ The SAP describes the Auditor's scope and methodology of the assessment. ▪ The SAP includes an attestation of the Auditor's independence. ▪ The SAP must be completed by the Auditor and submitted to CMS for review, prior to conducting the security and privacy controls assessment (SCA).
Security and Privacy Assessment Report (SAR)	▪ The SAR is not a living document; findings should not be added/removed from the SAR unless CMS' initial review of the final draft discovers deficiencies or inaccuracies that need to be addressed. ▪ The SAR should contain a summary of findings that includes ALL findings from the assessment, including documentation reviews, control testing, scanning, penetration testing, and interview(s). ▪ Explain if and how findings are consolidated. ▪ Ensure risk level determination is properly calculated, especially when weaknesses are identified as part of the Center for Internet Security (CIS) Top 20 and/or Open Web Application Security Project (OWASP) Top 10. ▪ Only one final SAR should be submitted to CMS. Once that SAR has been submitted and CMS has no additional comments or edits on the SAR, the prospective EDE Entity should not submit additional SARs.
Plan of Action and Milestones (POA&M)	▪ Ensure all open findings from the SAR have been incorporated into the POA&M. ▪ Explain if and how findings from the SAR were consolidated on the POA&M; include SAR reference numbers if applicable. ▪ Ensure the weakness source references each source in detail to include type of audit/assessment and applicable date range. ▪ Ensure the weakness description is as detailed as possible to include location/server/etc., if applicable. ▪ Ensure Scheduled Completion Dates, Milestones with dates, and appropriate risk levels are included. ▪ Monthly reviews and updates are required until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities described in the EDE SSP controls CA-5 and CA-7. Prospective EDE Entities can schedule their own time for monthly submissions of the POA&M, but must submit an update monthly to CMS until all significant or major findings are resolved. Thereafter, quarterly POA&M submissions are required as part of the ISCM activities.

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

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

Information Security and Privacy Continuous Monitoring (ISCM)

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

ISCM Requirements

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

ISCM Change Control

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

Common Controls

All EDE Entities (primary EDE Entities and upstream EDE Entities) are held to the same set of security and privacy requirements that are documented in the EDE SSP. CMS requires written confirmation from both the primary EDE Entity and upstream EDE Entity to allow a connection to CMS for an upstream entity.

- **Common Controls** are security or privacy controls whose implementation results in a security or privacy capability that is inheritable by multiple information systems being served by the primary EDE Entity. Upstream EDE Entities should leverage the common controls identified by the primary EDE Entity.
- **Security Control Inheritance** defines a situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application (i.e., entities either internal or external to the organization where the system or application resides).
- **Hybrid Control:** It is possible for an information system to inherit just part of a control from a primary EDE Entity, with the remainder of the control provided by the upstream EDE Entity. In this situation, both the primary EDE Entity and the upstream EDE Entity have a shared responsibility of implementing the full control objectives and implementation standards.

Common Controls (continued)

- Responsibility for implementing the following -1 controls (policies and procedures) cannot be inherited and must be described in some way by the upstream EDE Entity.
  - AC-1, Access Control
  - AT-1, Awareness and Training
  - CA-1, Security Assessment and Authorization
  - CP-1, Contingency Planning
  - IR-1, Incident Response
  - PS-1, Personnel Security
- For an EDE Entity to inherit a particular security or privacy control implemented by the primary EDE Entity, the following should be true:
  - The primary EDE Entity has designated the control as inheritable by documenting in the EDE SSP implementation description “inheritable.”
  - The primary EDE Entity has received RTC approval from CMS and evidence that the control is in fact operational with no major security weakness findings.

Additional Resources

- Guidelines for Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements: https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Guidelines-for-Third-party-Auditors-EDE-PY19PY20.pdf
- Processes and Guidelines for Becoming a Web-broker in the Federally-facilitated Exchange: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/Processes-Becoming-Web-broker.pdf
- FAQ: Enhanced Direct Enrollment Calendar Year 2019 Timeline: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Downloads/FAQ-EDE-CY2019.pdf
- FFE and FF-SHOP Enrollment Manual: https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Enrollment-Manual-062618.pdf
- List of approved EDE Entities (see "Enhanced Direct Enrollment Approved Partners"): https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Web-brokers-in-the-Health-Insurance-Marketplace.html
- Additional resources can be found on CCIIO's Web-broker Resources webpage: https://www.cms.gov/CCIIO/Programs-and-Initiatives/Health-Insurance-Marketplaces/Web-brokers-in-the-Health-Insurance-Marketplace.html
- 2019 Letter to Issuers: https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/2019-Letter-to-Issuers.pdf
- CMS website for issuers seeking certification to participate in the FFEs: https://www.qhpcertification.cms.gov/s/QHP
- CMS zONE:
  - CMS currently posts all technical information, guidelines, audit resources, and other documentation on the CMS zONE EDE Documents and Materials webpage at the following link: https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials. This webpage is accessible by members of the Private Issuer Community (for issuers) and the Web-Broker Community (for web-brokers) only.
- Help Desk Support:
  - Compliance and audit-related questions should be sent to the DE Help Desk at directenrollment@cms.hhs.gov
  - Technical issues or questions that concern technical build or system issues identified in the test or production environment should go to the FEPS Help Desk at CMS_FEPS@cms.hhs.gov

Acronyms

- A list of acronyms used in this presentation is available at the following link: https://www.regtap.info/uploads/library/EDE_Acronym_List_5CR_051618.pdf