



**Centers for Medicare & Medicaid Services
Federally Facilitated Marketplace
Contract HHSM-500-2015-00246C**

Enhanced Direct Enrollment (EDE) API Companion Guide

**Version 5.6
August 17, 2020**



consulting | technology | outsourcing

Document Control

Author	Version	Rev. date	Summary of Changes	Section	Page
Abigail Flock, Alexandra Astarita, Sean Song	1.0	1/23/2018	Initial Version	All	All
Scott Bickle, Alexandra Astarita, Sean Song	2.0	3/15/2018	Incorporated Client Feedback	All	All
Nikita Veera, Abigail Flock	3.0	10/22/2018	Updated Notice Retrieval Section Added HCV Section	8.2	13,14, 23, 24
Joshua Halsey	4.0	12/27/2018	Updates Throughout and Added Additional Sections	All	All
Joshua Halsey	4.1	1/25/2019	Added additional clarification to Section 6.4.1.1	6.4.1.1	13,14
James Stavely, Katherine Peters, Joshua Halsey	4.2	5/10/2019	Added Section 9.1.1, Added Section 12.1, Updated Section 15.1, Added Section 15.1.1, Added Section 15.2.1, Added Section 16, Added Section 17	9.1.1, 12.1, 15.1, 15.1.1, 15.2.1, 16, 17	20, 21, 24, 27, 28, 29, 30, 31, 32
Joshua Halsey	4.3	7/11/2019	Updated Section 16.2, Added Section 16.2.1, Added Section 16.2.2, Added Section 16.2.3	16.2, 16.2.1, 16.2.2, 16.2.3	31-35
Joshua Halsey	4.4	7/19/2019	Updated Section 5.1, Added Section 7.4.2	5.1, 7.4.2	7, 8, 19
Joshua Halsey	4.5	8/5/2019	Added Section 9.1.1	9.1.1	21-23
Joshua Halsey	4.6	9/9/2019	Added Sections 14.3 and 15.1.2	14.3, 15.1.2	31, 33-34

Author	Version	Rev. date	Summary of Changes	Section	Page
Joshua Halsey	4.7	12/3/2019	Added updated EDE end-to-end flow document to Section 1.2.1	1.2.1	1-2
Joshua Halsey	4.8	1/13/2020	Added Update Policy API to Section 1.2.4. Added Section 17 for the Update Policy API.	1.2.4, 17	5, 40-41
Joshua Halsey	4.9	1/14/2020	Updated Section 17 to include additional information related to cancellation/termination dates.	17	41
Joshua Halsey	5.0	1/16/2020	Updated Section 17 to include additional information related to PPS cancellation dates.	17	41
Joshua Halsey	5.1	3/24/2020	Added Section 3, including Subsections 3.1, 3.2, 3.3, and 3.4. Added Sections 6.1.1.1 and 17.3. Updated Sections 6.1.1, 15.2.1, and 17.2.	3, 3.1, 3.2, 3.3, 3.4, 6.1.1, 6.1.1.1, 15.2.1, 17.2, 17.3	5-11, 16, 42, 47-51
Joshua Halsey	5.2	4/1/2020	Added updated EDE flow document, including cancel/term and BAR opt-out functionality to Section 1.2.1. Clarifications to BAR opt-out business rules in Section 17.3. Added new RIDP and FARS endpoints to Sections 3.2.1.3 and 3.2.1.4.	1.2.1, 3.2.1.3, 3.2.1.4, 17.3	1, 8, 9, 49-51
Joshua Halsey	5.3	5/5/2020	Updated Section 9.1.1, to add clarification around allowable options for display of active and terminated policies.	9.1.1	27-28
Joshua Halsey	5.4	6/8/2020	Added Section 17.3.1, which includes example BAR opt-out messaging.	17.3.1	51-53
Joshua Halsey	5.5	7/19/2020	Made a number of updates to Section 15, including adding Section 15.1.1.1 and correcting guidance in Section 15.1.4.	15	39-42
Joshua Halsey	5.6	8/17/2020	Added Section 12.3, which includes guidance on SES optimistic locking errors.	12.3	36

Table of Contents

1	Introduction.....	1
1.1	Purpose.....	1
1.2	Overview.....	1
1.2.1	High-level End-to-End Flow.....	1
1.2.2	Consumer APIs.....	2
1.2.3	Eligibility APIs.....	3
1.2.4	Enrollment APIs.....	4
2	Assumptions.....	5
3	Basic API Usage Information.....	5
3.1	Data Services Hub (DSH) Onboarding.....	5
3.2	API Endpoints.....	5
3.3	API Headers.....	10
3.3.1	Role ID.....	10
3.3.2	User ID.....	11
3.3.3	Role ID and User ID for API Calls Made on Behalf of the EDE Entity.....	11
3.4	API Requests that Require a Prerequisite Store Permission or Store ID Proofing API Requests.....	11
4	ID Proofing.....	12
4.1	ID Proofing Overview.....	12
4.2	Store ID Proofing Service Flow.....	13
5	Permission.....	14
5.1	Permission Overview.....	14
5.2	Store Permission Record Service Flow.....	14
5.3	Consumer Revoke Permission.....	15
6	EDE Person Search.....	15
6.1	Person Search Overview.....	15
6.1.1	Agent/Broker (UI) Search vs. Consumer (Back-End) Search.....	16
6.2	Search Combinations.....	17
6.2.1	Minimum Search Criteria – EDE Consumer Flow.....	17
6.2.2	Minimum Search Criteria – EDE Agent/Broker Flow.....	17
6.3	Search Results.....	18
6.3.1	Person Search Response Data Elements.....	19
6.4	Determining Whether a New Application Needs to Be Created or Whether an Existing Application Should Be Used.....	20
6.4.1	When to Use an Existing Application.....	20
6.4.2	When to Create a New Application.....	21
7	Notice Retrieval.....	22
7.1	Notice Retrieval Overview.....	22
7.2	Searching for Metadata Record – Retrieving DSRS ID.....	22
7.3	Retrieving Notices.....	24
7.4	Form 1095-A Overview.....	24
7.4.1	Retrieving and Displaying Form 1095-A.....	25
7.4.2	Form 1095-A Notice Retrieval Testing.....	25
8	Document Upload.....	25

8.1	Document Upload Overview	25
8.2	Uploading a Document	26
8.3	Providing Document Feedback to Consumer	26
9	Get Enrollment.....	26
9.1	Get Enrollment Overview.....	26
9.1.1	UI Display of Get Enrollment Data.....	27
9.1.2	EDE Issuers – Using Get Enrollment as a Standalone Tool	30
10	DMI.....	32
10.1	DMI Overview	32
10.2	Consolidated Status.....	33
11	SVI.....	33
11.1	SVI Overview	33
11.2	Consolidated Status.....	34
12	Standalone Eligibility Services (SES)	35
12.1	SES Overview.....	35
12.2	Health Coverage Verification	35
12.3	Optimistic Locking	36
13	Payment Redirect	37
13.1	Payment Redirect Overview	37
13.2	Payment Redirect Response.....	37
13.3	Payment Redirect Integration Requirements	38
14	Legacy DE Services – Fetch Eligibility and Submit Enrollment	39
14.1	Fetch Eligibility	39
14.1.1	Variable Eligibility Data	39
14.1.2	Plan Category Limitations (aka Metal Level Plan Restrictions).....	40
14.1.3	Get App Address Requirement – Phase 3 EDE Entities Only	41
14.1.4	Allocation of APTC to Enrollment Groups.....	41
14.2	Submit Enrollment.....	42
15	Event-Based Processing (EBP).....	42
15.1	Event-Based Processing Overview	42
15.2	Email Toggle Functionality	43
15.2.1	EDE Requests to Disable FFM-Generated Emails	43
15.2.2	EDE Entity Email Requirements and Recommended Best Practices	44
15.2.3	Email Groups.....	46
16	Update Policy.....	47
16.1	Update Policy Overview	47
16.2	Update Policy API – Cancellation/Termination Business Rules.....	48
16.3	Update Policy API – BAR Opt-Out Business Rules	49
16.3.1	BAR Opt-Out Messaging	51
17	Performance Testing	54
17.1	Performance Testing Overview	54

1 Introduction

1.1 Purpose

The Enhanced Direct Enrollment (EDE) API Companion Guide serves as a reference guide to assist an EDE entity with their EDE Application Program Interface (API) integration process. This document will outline the intent of the EDE initiative as well provide high-level, and in some instances detailed, information on the use of each EDE API. This document is not intended to be the sole source of documentation outlining EDE API integration requirements, and instead is intended to serve as a compliment to the other EDE integration documentation that is available on zONE at <https://zone.cms.gov/document/enhanced-direct-enrollment-edo-documents-and-materials>.

1.2 Overview

Classic Direct Enrollment (DE) is a means by which private entities, such as web-brokers and issuers, provide a plan shopping and enrollment experience for consumers as an alternative to HealthCare.gov, while offering the same benefits and subsidies as the Marketplace. Currently, DE entities use the HealthCare.gov Classic DE program to facilitate enrollments in two ways: 1) they provide a shopping and enrollment experience directly to consumers through their own branded website, or 2) they provide a platform or type of portal for agents or brokers to use when assisting consumers in shopping for and enrolling in coverage. When using Classic DE, the eligibility application is completed on HealthCare.gov, and then the consumer or agent/broker uses plan comparison tools on the DE entity's site to shop for and select a plan. This current process is referred to as a "double-redirect" because when an eligibility determination is required, the consumer is first directed from the DE entity website to HealthCare.gov, and then when the eligibility information is entered and the eligibility determination made, the consumer is redirected back to the DE entity website for plan selection and enrollment.

Enhanced Direct Enrollment addresses the pain points faced in the current Classic "double-redirect" DE process. EDE uses an API-based approach, which allows EDE entities to facilitate not only the plan shopping and enrollment experience, but also allows EDE entities to facilitate the eligibility application process and post-enrollment activities. Below, readers will find information pertaining to each EDE API.

1.2.1 High-level End-to-End Flow

Below is the high-level end-to-end workflow for the EDE process. This process depicts the various frontend and backend interactions for EDE. The flow represents the recommended high-level process for the EDE user experience.



EDE_FEBE
flows_20200320.pdf

1.2.2 Consumer APIs

Consumer APIs enable stakeholders to search for, modify, store, upload, and retrieve consumer data. These APIs are not specific to the eligibility application or enrollment.

The table below outlines the consumer APIs that are available.

Table 1-1 - Consumer APIs

API	Business Capability
Person Search	This service allows for a stakeholder to search for a consumer's existing application within the FFE. A user may search for a person using a specific set of data, outlined later in this document.
Get DMI	This service provides a high-level overview of any Data Matching Issues (DMIs) tied to a consumer. A DMI is created when a consumer attestation does not match data returned from a trusted data source during eligibility determinations. A DMI may affect a consumer's ability to enroll in a Qualified Health Plan (QHP). Consumers have a certain timeframe in which to resolve DMIs, which is captured in a timer.
Get SVI	This service provides a high-level overview of any Special Enrollment Period (SEP) Verification Issues (SVIs) tied to a consumer. An SVI is created when a consumer attests to being eligible for a SEP that requires verification. A consumer may be required to upload documentation proving that he or she is eligible to be granted the SEP. Consumers have a certain timeframe in which to resolve SVIs, which is captured in a timer.
Store Permission	This service is used to store a set of required data when a consumer has authorized an EDE entity or agent/broker to submit API transactions on his or her behalf.
Revoke Permission	This service is used when a consumer wants to revoke the authorization for an EDE entity or agent/broker to submit API transactions on his or her behalf
Store ID Proofing	This service is used to store a set of required data when a consumer has successfully ID proofed at the EDE entity.
Document Upload	This service provides the capability to store documents and corresponding metadata. For EDE, consumers may upload documents through an EDE entity to resolve either a DMI or an SVI.
Notice Retrieval	This service allows authorized EDE entities to retrieve consumer notices directly from the FFE document storage via a time-expiring URL.
Metadata Search	This service provides the capability to search for metadata records tied to a consumer. This service will return metadata for notices tied to a consumer.

API	Business Capability
Payment Redirect	This API allows stakeholders to redirect a consumer to their issuer's payment website for their binder payment.
Event-Based Processing	This API allows EDE entities to ingest certain events for consumers as they occur, and subsequently enables EDE entities to distribute corresponding communications to their consumers.

1.2.3 Eligibility APIs

Eligibility APIs enable stakeholders to create, update, view, or submit a Consumer's application without ever going to the Exchange. The Eligibility APIs also enable stakeholders to retrieve and determine eligibility for Exchange coverage; this includes eligibility for Medicaid, Children's Health Insurance Program (CHIP), Advance Premium Tax Credits (APTC), Cost Sharing Reductions (CSR), and Qualified Health Plans (QHPs). These APIs are primarily meant for EDE flows, but some APIs may be exposed to additional external stakeholders.

Table 1-2 - Eligibility APIs

API	Business Capability
Create Application	This API is used to create an initial application for a consumer.
Create Application from Prior Year Application	This API is used to create a prepopulated application for a consumer from a prior year application.
Update Application	This API to modify or update an existing application, based on updates to attestations by the requestor.
Add Member	This API is used to add members to an application.
Remove Member	This API is used to remove members from an application.
Submit Application	This API allows a user to finalize and submit an application. The service computes and/or re-computes events to ensure that all required fields are present and valid as required to submit the application. Upon successful submission, the service generates a submitted application that is immutable and can be used to process enrollment and other downstream processes.

API	Business Capability
Get Application Summary	This API provides a summary view of an insurance application.
Get Application Detail	This API provides a detailed view of the insurance application, including member and application-level attestations, verifications, and final eligibility determination results.
System Reference Data	This API provides system configuration data.
State Reference Data	This API provides state configuration data.
Delete Application	This API can be used to delete an application that does not have an enrollment tied to it.
Fetch Eligibility	This API allows stakeholders to retrieve consumer eligibility and enrollment information.
Remote Identity Proofing (RIDP)	This API allows EDE entities to remotely identity proof consumers in the EDE consumer flow, and to remotely identity proof agents/brokers before they use an EDE agent/broker flow. This is an Experian service that flows through the Data Services Hub (DSH).
Fraud Archive Reporting Service (FARS)	This API allows EDE entities to confirm remote identity proofing has successfully occurred for a consumer or agent/broker at the Experian Call Center. This is an Experian service that flows through the Data Services Hub (DSH).

1.2.4 Enrollment APIs

Enrollment APIs provide EDE entities with the ability to retrieve and create enrollment data in real time.

Table 1-3 - Enrollment APIs

API	Business Capability
Get Enrollment	This API allows EDE entities to retrieve enrollment data for a consumer in real-time.
Submit Enrollment	This API allows an EDE entity to submit an enrollment.

API	Business Capability
Update Policy	This API allows an EDE entity to initiate certain actions that impact a consumer's existing policy or Pended Plan Selection (PPS). Functionality available via the Update Policy API currently includes cancellation, termination, and Batch Auto-Renewal (BAR) opt-out functionality.

2 Assumptions

1. As noted in the introduction section, the EDE API Companion Guide serves as a reference guide to assist an EDE entity with their EDE Application Program Interface (API) integration process. This document will outline the intent of the EDE initiative as well provide high-level, and in some instances detailed, information on the use of each EDE API. This document however is not intended to be the sole source of documentation outlining EDE API integration requirements, and instead is intended to serve as a compliment to the other EDE integration documentation that is available on zONE at <https://zone.cms.gov/document/enhanced-direct-enrollment-edo-documents-and-materials>.
2. The EDE API Companion Guide is subject to change based on the evolving functionality for the various EDE APIs.

3 Basic API Usage Information

3.1 Data Services Hub (DSH) Onboarding

In order for EDE entities to get access to the Classic DE or EDE services, EDE entities will need to complete a Hub Onboarding Form which is available on zONE at <https://zone.cms.gov/document/hub-onboarding-form>. The Hub Onboarding Form should be submitted to Hubsupport@sparksoftcorp.com. Once the Hub Onboarding Form is submitted, DSH will enable UAT0 access for the requested services; UAT0 is the FFE's partner testing environment. UAT0 access is generally enabled within 2-3 business days after submission of the Hub Onboarding Form.

EDE entities should note that production access will only be granted once an entity has received formal Classic DE or EDE approval. For EDE production access in particular, CMS will reach out to the approved EDE entities to coordinate a formal go live date and time.

3.2 API Endpoints

The below sections include the endpoints that EDE entities will use for the Classic DE and EDE services. EDE entities should note that their API requests are sent to the Data Services Hub (DSH), where the DSH subsequently routes the API requests to the FFE, or in the case of the

RIDP and FARS APIs, to Experian. Accordingly, EDE entities should use the appropriate DSH endpoints below when submitting API requests to the FFE or Experian, and should refrain from using any other published endpoints, such as any FFE endpoints included in the EDE API Spec extracts available on zONE at <https://zone.cms.gov/document/enhanced-direct-enrollment-edo-documents-and-materials>. If an EDE entity uses non-DSH endpoints to submit API requests, the transactions will fail.

3.2.1.1 Classic DE Pathway – UAT0

EDE entities that wish to connect to the Classic DE pathway in our partner testing environment, UAT0, will need to open the English and Spanish cookies below in separate tabs in a web browser, and then must post the necessary SAML to the appropriate secure redirect page in a third tab in the same web browser. The SAML specifications are outlined in the DE API Specs document available on zONE at <https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials>.

Once the Classic DE redirect occurs, the user will be routed to the consumer or agent/broker login page, based on the user type that is provided in the SAML. On the consumer login page, the user can either create a new consumer account or access an existing consumer account. When creating new consumer accounts via the Classic DE pathway in UAT0, EDE entities must use the RIDP data available on zONE at <https://zone.cms.gov/document/all-issuer-testing-materials>. Note that this is different RIDP data than what is used to test the RIDP and FARS APIs. Once the RIDP portion of the consumer account creation process is passed, EDE entities can anonymize the consumer data as desired on the eligibility application, with the exception of the SSN. EDE entities should either not enter an SSN when completing the eligibility application in the test environment, or should use an SSN from one of the many CMS test scenarios that are available on zONE, such as an SSN from the API Functional Integration Toolkit test data. While SSNs from available test scenarios can be used for testing, EDE entities should always anonymize the first name, last name, date of birth, street address, and email address for members on the eligibility application when testing, in order to prevent running into PTN-related issues, such as SVIs or DMIs not generating as expected.

After submitting the eligibility application, users will be able to redirect back to the EDE entity's site to complete plan shopping. The EDE entity will utilize the Fetch Eligibility API to retrieve the consumer's eligibility results, and will use the Submit Enrollment API to finalize the consumer's enrollment. The Fetch Eligibility and Submit Enrollment API endpoints may also be used when testing the EDE pathway.

If an EDE entity would like to test the Classic DE agent/broker pathway, the EDE entity will need to use valid agent/broker test credentials when logging into that pathway. If an EDE entity needs to request agent/broker test credentials, they can do so by emailing IssuerAssistanceTesting@bah.com. If agent/broker test credentials are issued to an EDE entity, the EDE entity should go to portalval.cms.gov to reset the password for the credentials.

Below is the information that is applicable to connecting to the Classic DE pathway in UAT0:

- English Cookie: <https://uat0.healthcare.gov/?ACA=kbV0uKB8cG>
- Spanish Cookie: <https://uat0.cuidadodesalud.gov/?ACA=bNvHvLuymF>
- Secure Redirect: <https://uat0.healthcare.gov/marketplace/brokerService>

-
- Spanish Secure Redirect: <https://uat0.cuidadodesalud.gov/marketplace/espBrokerService>
 - Fetch Eligibility API: <https://impl.hub.cms.gov/ApplicantEligibilityServiceV4>
 - Submit Enrollment API: <https://impl.hub.cms.gov/ApplicantEnrollmentServiceV4>
 - Applicable certificates, which are available on zONE:
 - UAT0 FFE Gateway Certificate: <https://zone.cms.gov/document/ffm-gateway-certificates>
 - Required if validating the FFE certificate in the redirect SAML that is posted to the EDE entity's return URL.
 - UAT0 DSH Gateway Certificate: <https://zone.cms.gov/document/hub-impl-certificate-update>
 - Required if the EDE entity trusts the "impl.hub.cms.gov" server certificate, the root certificate authority certificate, or the intermediate certificate authority certificate associated with the EDE APIs.

EDE entities should note that the UAT0 English and Spanish cookies change each year, prior to the start of all-partner OE testing. The new cookies will subsequently not be added to the EDE API Companion Guide until after the new year's plan data becomes publically available, which usually occurs in mid to late October. In order for EDE entities to obtain the new cookies prior to the new year's plan data becoming publically available, EDE entities need to complete a Confidentiality Agreement. Details related to the Confidentiality Agreement are generally socialized to partners during the Tuesday Issuer Technical Workgroup call, which is open to all partners.

3.2.1.2 Classic DE Pathway – Production

EDE entities that wish to connect to the Classic DE pathway in production can do so by posting the necessary SAML to the appropriate secure redirect page. The required SAML is outlined in the DE API Specs document available on zONE at <https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials>. Note that unlike UAT0, connecting to the Classic DE pathway in production does not require opening English and Spanish cookies. Note as well, only approved entities that have been granted production access will be able to connect to the Classic DE services in production.

Below is the information that is applicable to connecting to the Classic DE pathway in production:

- English Secure Redirect: <https://www.healthcare.gov/marketplace/brokerService>
- Spanish Secure Redirect: <https://www.cuidadodesalud.gov/marketplace/espBrokerService>
- Fetch Eligibility: <https://hub.cms.gov/ApplicantEligibilityServiceV4>
- Submit Enrollment: <https://hub.cms.gov/ApplicantEnrollmentServiceV4>
- Applicable certificates, which are available on zONE:
 - Production FFE Gateway Certificate: <https://zone.cms.gov/document/ffm-gateway-certificates>
 - Required if validating the FFE certificate in the redirect SAML that is posted to the EDE entity's return URL.

-
- Production DSH Gateway Certificate:
 - Issuers: <https://zone.cms.gov/document/dsh-production-certificate-de-issuers>
 - Web-brokers: <https://zone.cms.gov/document/dsh-production-certificate-de-web-brokers>
 - Required if the EDE entity trusts the “hub.cms.gov” server certificate, the root certificate authority certificate, or the intermediate certificate authority certificate associated with the EDE APIs.

3.2.1.3 EDE API Endpoints – UAT0

Below are the endpoints that EDE entities will use when testing the EDE APIs in UAT0. Similar to Classic DE pathway testing, EDE entities should either refrain from using SSNs when completing eligibility applications via the EDE APIs, or alternatively use SSNs from one of the many CMS eligibility application test scenarios that are available on zONE, such as SSNs from the API Functional Integration Toolkit test data. While SSNs from available eligibility application test scenarios can be used for testing, EDE entities should always anonymize the first name, last name, date of birth, street address, and email address for members on the eligibility application when testing, in order to prevent running into PTN-related issues, such as SVIs or DMIs not generating as expected. EDE entities should also be aware that the RIDP and FARS API test data available on zONE at <https://zone.cms.gov/document/enhanced-direct-enrollment-edo-documents-and-materials>, is not in sync with the FFE test harness data, and the RIDP and FARS API test data can therefore only be used when testing those APIs.

Please find the UAT0 endpoints for the EDE APIs below:

- RIDP API: <https://impl.hub.cms.gov/RIDPServiceDE>
 - RIDP API, starting 5/18/2020: <https://impl.hub.cms.gov/RIDPService>
- FARS API: <https://impl.hub.cms.gov/FARSServiceDEV3>
 - FARS API, starting 5/18/2020: <https://impl.hub.cms.gov/FARSService>
- Store ID Proofing API: <https://impl.hub.cms.gov/ede/v1/identity-proofing-records> (POST)
- Person Search API: <https://impl.hub.cms.gov/ede/v1/get-persons> (POST)
- Create Application API: <https://impl.hub.cms.gov/ses/v1/applications> (POST)
- Create App From Prior Year App API:
<https://impl.hub.cms.gov/ses/v1/createApplicationFromPriorYear> (POST)
- Store Permission API: <https://impl.hub.cms.gov/ses-permissions/v1/permission> (POST)
- Revoke Permission API: <https://impl.hub.cms.gov/ses-permissions/v1/permission> (PUT)
- Get Application API: <https://impl.hub.cms.gov/ses/v1/applications> (GET)
- Add Member API: [https://impl.hub.cms.gov/ses/v1/applications/\[APP_ID\]/members](https://impl.hub.cms.gov/ses/v1/applications/[APP_ID]/members) (POST)
- Remove Member API: [https://impl.hub.cms.gov/ses/v1/applications/\[APP_ID\]/members](https://impl.hub.cms.gov/ses/v1/applications/[APP_ID]/members) (DELETE)
- Update Application API: [https://impl.hub.cms.gov/ses/v1/applications/\[APP_ID\]](https://impl.hub.cms.gov/ses/v1/applications/[APP_ID]) (PUT)
- Submit Application API: [https://impl.hub.cms.gov/ses/v1/applications/\[APP_ID\]/submissions](https://impl.hub.cms.gov/ses/v1/applications/[APP_ID]/submissions) (POST)
- Get SVI API: <https://impl.hub.cms.gov/ede/v1/get-sep-verification-issues> (POST)

- Get DMI API: <https://impl.hub.cms.gov/v1/get-data-matching-issues> (POST)
- Metadata Search API: <https://impl.hub.cms.gov/dsrs/v1/search-metadata> (POST)
- Notice Retrieval API: [https://impl.hub.cms.gov/dsrs/v1/documents/\[DSRS_ID\]](https://impl.hub.cms.gov/dsrs/v1/documents/[DSRS_ID]) (GET)
- Document Upload API: <https://impl.hub.cms.gov/dsrs-docupload/v1/documents> (POST)
- Payment Redirect API: [https://impl.hub.cms.gov/ies/v1/payment-redirects?applicationId=\[APP_ID\]](https://impl.hub.cms.gov/ies/v1/payment-redirects?applicationId=[APP_ID]) (GET)
- Get Enrollment API: <https://impl.hub.cms.gov/ede/v1/get-policies> (POST)
- Update Policy API: <https://impl.hub.cms.gov/ede-ies/v1/policies> (PUT)
- State Reference Data API: [https://impl.hub.cms.gov/ses/v1/reference-data/states/\[STATE_CODE\]](https://impl.hub.cms.gov/ses/v1/reference-data/states/[STATE_CODE]) (GET)
- System Reference Data API: <https://impl.hub.cms.gov/ses/v1/reference-data/system> (GET)
- Delete Application API: [https://impl.hub.cms.gov/ses/v1/applications/\[APP_ID\]](https://impl.hub.cms.gov/ses/v1/applications/[APP_ID]) (DELETE)
- Event-Based Processing API – Verification Issues: https://impl.hub.cms.gov/ebs/v1/events?q=verification_issues (GET)
- Event-Based Processing API – Applications: <https://impl.hub.cms.gov/ebs/v1/events?q=applications> (GET)
- Event-Based Processing API – Enrollments: <https://impl.hub.cms.gov/ebs/v1/events?q=enrollments> (GET)
- Event-Based Processing API – Consumer Information: https://impl.hub.cms.gov/ebs/v1/events?q=consumer_information (GET)

3.2.1.4 EDE API Endpoints - Production

Below are the endpoints that EDE entities will use when connecting to the EDE APIs in production:

- RIDP API: <https://hub.cms.gov/RIDPServiceDE>
 - RIDP API, starting 6/14/2020: <https://hub.cms.gov/RIDPService>
- FARS API: <https://hub.cms.gov/FARSServiceDEV3>
 - FARS API, starting 6/14/2020: <https://hub.cms.gov/FARSService>
- Store ID Proofing API: <https://hub.cms.gov/ede/v1/identity-proofing-records> (POST)
- Person Search API: <https://hub.cms.gov/ede/v1/get-persons> (POST)
- Create Application API: <https://hub.cms.gov/ses/v1/applications> (POST)
- Create App from Prior Year App API: <https://hub.cms.gov/ses/v1/createApplicationFromPriorYear> (POST)
- Store Permission API: <https://hub.cms.gov/ses-permissions/v1/permission> (POST)
- Revoke Permission API: <https://hub.cms.gov/ses-permissions/v1/permission> (PUT)
- Get Application API: <https://hub.cms.gov/ses/v1/applications> (GET)
- Add Member API: [https://hub.cms.gov/ses/v1/applications/\[APP_ID\]/members](https://hub.cms.gov/ses/v1/applications/[APP_ID]/members) (POST)
- Remove Member API: [https://hub.cms.gov/ses/v1/applications/\[APP_ID\]/members](https://hub.cms.gov/ses/v1/applications/[APP_ID]/members) (DELETE)
- Update Application: [https://hub.cms.gov/ses/v1/applications/\[APP_ID\]](https://hub.cms.gov/ses/v1/applications/[APP_ID]) (PUT)
- Submit Application: [https://hub.cms.gov/ses/v1/applications/\[APP_ID\]/submissions](https://hub.cms.gov/ses/v1/applications/[APP_ID]/submissions) (POST)

-
- Get SVI DMI: <https://hub.cms.gov/ede/v1/get-sep-verification-issues> (POST)
 - Get DMI API: <https://hub.cms.gov/ede/v1/get-data-matching-issues> (POST)
 - Metadata Search: <https://hub.cms.gov/dsrs/v1/search-metadata> (POST)
 - Notice Retrieval: [https://hub.cms.gov/dsrs/v1/documents/\[DSRS_ID\]](https://hub.cms.gov/dsrs/v1/documents/[DSRS_ID]) (GET)
 - Document Upload: <https://hub.cms.gov/dsrs-docupload/v1/documents> (POST)
 - Payment Redirect: [https://hub.cms.gov/ies/v1/payment-redirects?applicationId=\[APP_ID\]](https://hub.cms.gov/ies/v1/payment-redirects?applicationId=[APP_ID]) (GET)
 - Get Enrollment: <https://hub.cms.gov/ede/v1/get-policies> (POST)
 - Update Policy API: <https://hub.cms.gov/ede-ies/v1/policies> (PUT)
 - State Reference Data API: [https://hub.cms.gov/ses/v1/reference-data/states/\[STATE_CODE\]](https://hub.cms.gov/ses/v1/reference-data/states/[STATE_CODE]) (GET)
 - System Reference Data API: <https://hub.cms.gov/ses/v1/reference-data/system> (GET)
 - Delete Application API: [https://hub.cms.gov/ses/v1/applications/\[APP_ID\]](https://hub.cms.gov/ses/v1/applications/[APP_ID]) (DELETE)
 - Event-Based Processing API – Verification Issues: https://hub.cms.gov/ebs/v1/events?q=verification_issues (GET)
 - Event-Based Processing API – Applications: <https://hub.cms.gov/ebs/v1/events?q=applications> (GET)
 - Event-Based Processing API – Enrollments: <https://hub.cms.gov/ebs/v1/events?q=enrollments> (GET)
 - Event-Based Processing API – Consumer Information: https://hub.cms.gov/ebs/v1/events?q=consumer_information (GET)

3.3 API Headers

EDE entities should note that their API requests are sent to the Data Services Hub (DSH), where the DSH subsequently routes the API requests to the FFE, or in the case of the RIDP and FARS APIs, to Experian. Accordingly, EDE entities should ensure they are using the correct API request headers when sending transactions to the FFE through the DSH. The API request headers that EDE entities should use are outlined in the DSH Business Service Definitions (BSDs) available on zONE at <https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials>. EDE entities should refrain from using any other published headers, such as any FFE headers included in the EDE API Spec extracts available on zONE at <https://zone.cms.gov/document/enhanced-direct-enrollment-ede-documents-and-materials>. If an EDE entity uses non-DSH headers to submit API requests, the transactions will fail.

3.3.1 Role ID

The JSON-based EDE APIs will all include a Role ID header element, which will either be AGENT_BROKER for an EDE agent/broker pathway transaction, or CONSUMER_DE for an EDE consumer pathway transaction. For EDE API requests being sent to the System Reference Data, State Reference Data, and Event-Based Processing APIs, these API requests are being made on behalf of the EDE entity and not on behalf of an individual consumer or agent/broker, and the EDE entity should always use a CONSUMER_DE value for these transactions.

EDE entities should also be aware that the XML-based Fetch Eligibility and Submit Enrollment APIs also include a similar field within the body of their API requests. Specifically, EDE entities will always need to provide a PartnerWebSiteUserCode value of either EDEConsumer for EDE consumer pathway transactions, or EDEAgent for EDE agent/broker pathway transactions, when submitting Fetch Eligibility and Submit Enrollment API requests.

3.3.2 User ID

The JSON-based EDE APIs will all include a User ID header element. For EDE consumer pathway transactions, the User ID should always be either the User ID for the consumer on the EDE entity's site, or some other unique identifier that the EDE entity assigns to the consumer if consumer account creation is not required on the EDE entity's site. For EDE agent/broker pathway transactions, the User ID should always be the actual FFE User ID for the agent/broker. In the production environment, the FFE User ID for an agent/broker will be the same User ID that the agent/broker uses to log into the Classic DE pathway and to portal.cms.gov; the EDE entity will need to collect this information from their agents/brokers if offering an agent/broker pathway. In the testing environment, the agent/broker User ID provided in the header of the API request will need to be a valid testing agent/broker FFE User ID. If an EDE entity needs to request agent/broker credentials for the test environment, they can do so by reaching out to IssuerAssistanceTesting@bah.com. If agent/broker test credentials are issued to an EDE entity, the EDE entity should go to portalval.cms.gov to reset the password for the credentials.

3.3.3 Role ID and User ID for API Calls Made on Behalf of the EDE Entity

EDE entities should note that there are certain API calls that will be made on behalf of the EDE entity system, instead of on behalf of a consumer or agent/broker. Specifically, calls to the System Reference Data API, the State Reference Data API, and the Event-Based Processing API will all be made on behalf of the EDE entity system. For these APIs, EDE entities are required to use the CONSUMER_DE Role ID, and are also required to use a User ID that represents the EDE entity's system. For example, an EDE entity calling the System Reference Data API might use a User ID of "EDEPartnerXSystem" to indicate that the API call is being made on behalf of the EDE entity.

3.4 API Requests that Require a Prerequisite Store Permission or Store ID Proofing API Requests

EDE entities should be aware that many of the EDE APIs require that the EDE entity have permission stored via the Store Permission API, before they can make a successful API request. EDE entities should also note that the Store Permission request will require a prerequisite Store ID Proofing API call, when storing permission in the consumer or in-person agent/broker flows. If an EDE entity has not made the prerequisite Store Permission and Store ID Proofing API request when applicable, subsequent API requests to other EDE APIs may fail due to the lack of permission. The only EDE APIs that don't require a prerequisite Store Permission API call are the RIDP, FARS, Store ID Proofing, Person Search, Create App, Create App from Prior Year App, System Reference Data, and State Reference Data APIs.

4 ID Proofing

4.1 ID Proofing Overview

In order for a consumer to submit an insurance application to receive an eligibility determination through an EDE entity, the primary applicant on the application must be ID proofed¹. This should happen prior to the entity attesting that the consumer has granted the entity permission to work on his or her behalf.

A primary applicant will only have to be identity proofed by a given EDE entity once, as long as the EDE entity requires the consumer to create an account on their site, and tracks that ID proofing for the consumer occurred. ID proofing records will span the lifetime of a consumer's relationship with an EDE entity, including if the consumer leaves to work with another EDE entity and returns at a later time (in this scenario, the consumer would have to be ID proofed with the new EDE entity, if the new entity hadn't previously ID proofed the consumer). The ID proofing record can also be used across multiple applications with the same entity, again, as long as the EDE entity requires the consumer to create an account on their site, and the entity can maintain a record of the ID proofing across applications. However, if an EDE entity receives a new consumer that has not previously been ID proofed with the entity, the entity must ID Proof the consumer, even if the consumer has an existing application or enrollment with a different EDE entity or the FFM.

ID proofing may occur either online or offline. Online ID proofing will occur in the EDE consumer flow, while offline ID proofing will occur in the in-person agent/broker flow. Offline ID proofing is not currently required in the agent/broker telephone flow, but is required in the in-person agent/broker flow. In the in-person agent/broker flow, a consumer will provide documentation to an agent/broker that will provide proof of his or her identity; the documentation does not need to be uploaded, however the agent/broker will need to enter identifying information for the documentation used to verify a consumer's identity. In the online flow, the EDE entity will use a third-party authentication provider, such as Experian, to verify the consumer's identity. Note that CMS makes its Experian RIDP and FARS services available for EDE entity use in the online flow. If an EDE entity elects to use a third-party identity proofing service (i.e. not the CMS RIDP and FARS services) for the online flow, the entity must have their auditor evaluate and certify that the service is Federated Identity, Credential, and Access Management (FICAM) Trust Framework Solutions (TFS) approved and that the EDE entity has implemented the service correctly. EDE entities using a third-party identity proofing service must also be able to produce documentary evidence that each applicant has been successfully identity proofed, at CMS' request. Documentation related to a third-party identity proofing service may be requested in an audit or investigation by CMS.

EDE entities must provide the following data to the Store ID Proofing API regardless of whether the consumer was ID proofed through the online consumer flow or the offline in-person agent/broker flow:

¹ In the case of a minor, the adult present on the application will need to be ID proofed. In the case of an emancipated minor, the emancipated minor will need to be ID proofed.

-
- Identity Proofing Channel Type
 - Identity Proofing Method Type
 - First Name
 - Last Name
 - Birth Date

If a consumer's identity is verified in the in-person agent/broker flow, in addition to the fields above, the EDE Entity should provide the following data to the Store ID Proofing Record API:

- Identity Proofing Document Type
- Identity Proofing Document Identifier
- National Producer Number

If a consumer's identity is verified online in the consumer flow, the EDE entity should also provide the following data to the Store ID Proofing API:

- Online Transaction Identifier

The fields above will be stored as part of an ID proofing record request. Additionally, the Partner ID of the EDE entity making the request, as well as an Identity Proofing Identifier (created as part of the Store ID Proofing API transaction), will be stored with each record. Upon successful storage of an ID proofing record, the Store ID Proofing API will return the Identity Proofing Identifier to the EDE entity, which must be stored by the EDE entity. This identifier will be provided in subsequent calls to the Permission API, as described below.

Note, if a consumer is identity proofed in-person in the agent/broker flow, the consumer must provide specific documentation to prove their identity. The documentation provided does not need to be uploaded by the agent/broker, however the agent/broker will need to provide identifying information for the documentation used to verify a consumer's identity. The accepted documentation for in-person ID proofing is outlined in the embedded document below.



4.2 Store ID Proofing Service Flow

Prior to attesting that a consumer has granted an EDE entity permission to work on his or her behalf, an EDE entity should provide an identity proofing record to the FFM. When the identity proofing record is successfully stored, the Store ID Proofing API will return an Identity Proofing Identifier to the EDE entity. In order to successfully store a permission attestation, the Identity Proofing Identifier must be provided as part of the write request to the Store Permission API. The Store Permission API will then verify that the Partner ID of the entity making the permission request matches the Partner ID associated with the identity proofing record. If the Partner IDs match, the permission record will be stored. If the Partner ID of the identity proofing record does not match the Partner ID of the permission request, the EDE entity will not be able to complete any actions that require permission.

5 Permission

5.1 Permission Overview

In order for a consumer to submit an eligibility application to receive an eligibility determination through an EDE entity, the consumer must provide permission to the EDE entity to work on their behalf. The EDE Store Permission API is used to store acknowledgment of consumer permission in the FFM. This allows an EDE entity to work on the consumer's behalf and is applicable to two EDE flows:

- **Consumer Flow:** Through an EDE entity website, a consumer can provide permission to the EDE entity to work on their behalf prior to claiming an existing application, or starting a new application. EDE entities must include a permission attestation within their UI, which the consumer must attest to before the EDE entity stores permission via the Store Permission API.
- **Agent/Broker Flow:** In the agent/broker flow, a consumer provides verbal or written permission to the agent/broker to allow the EDE entity and agent/broker to work on their behalf. The agent/broker must attest to having received permission to work on behalf of the consumer within the EDE entity's UI, prior to a Person Search API call occurring. If an EDE entity makes a Person Search UI component available for agents/brokers, the EDE entity must include an attestation on the Person Search UI page that the agent/broker is required to attest to, prior to a Person Search API call occurring. Note, while the UI attestation must occur prior to a Person Search API call occurring, the actual Store Permission API call must occur after both: 1) the Person Search API call, and 2) the agent/broker either claiming an existing application, [when applicable](#), or creating a new application via the Create App API.

Each EDE entity the consumer interacts with must receive permission from the consumer and call the Store Permission API to store the permission data in the FFM. However, only one EDE entity can hold permission on an application at any given time. Therefore, if a consumer switches to a new EDE entity (aka "Partner Switching"), permission is then established with the new EDE entity and permission is revoked from the prior EDE entity.

EDE entities must also provide "Revoke Permission" functionality on their website via the FFM Revoke Permission API. This API allows a consumer to revoke permission from the EDE entity to work on their behalf, without requiring a consumer to switch EDE entities to do so.

5.2 Store Permission Record Service Flow

The action of obtaining a consumer's permission falls under the responsibility of the EDE entity. Prior to obtaining inputs to be passed to the Store Permission API, EDE entities must complete ID proofing and comply with CMS provided guidelines on how permission is received from a consumer in both offline and online scenarios.

To properly use the Store Permission API, the EDE entities must provide functionality that allows the Store Permission API to be accessed for both the agent/broker flow and consumer flow.

Once Permission has been received from the consumer according to CMS guidelines, the EDE entity must provide the following inputs to successfully call the Store Permission API:

- Identity Proofing Identifier
- Identity Proofing Channel
- Insurance Application Identifier
- National Producer Number (Optional)

The Store Permission API will complete a set of validations and, if all validations pass, will store permission data to the FFM and return a successful response.

5.3 Consumer Revoke Permission

The Revoke Permission API allows a consumer to revoke permission from an EDE entity via the EDE entity website.

To properly use the Revoke Permission API, EDE entities must provide functionality that allows the consumer to request permission revocation via the consumer's account on the EDE entity's website.

If a consumer decides to revoke permission, the EDE entity must provide the following inputs to successfully call the Revoke Permission API:

- Insurance Application Identifier

The Revoke Permission API will complete a set of validations and if all pass, permission will be marked as revoked for the EDE entity and a successful response will be returned to the EDE entity. The EDE entity will no longer be able to work on behalf of the consumer in the FFM unless the consumer once again grants permission to the EDE entity and the Store Permission API is called again.

If any validations fail, the FFM will not process the revocation and an error response will be returned to the EDE entity.

6 EDE Person Search

6.1 Person Search Overview

The EDE Person Search API will allow EDE entities to input consumer demographic information in order to retrieve a consumer's existing application(s). EDE entities must always complete a Person Search to determine whether a consumer has an existing application that can be used, prior to creating a new application for a consumer. This requirement is not only applicable to the consumer flow, but also to the agent/broker flow. Agents/Brokers must also be required to search for an existing application, prior to creating a new application. EDE entities should never allow a new application to be created if there is an existing application returned by the Person Search API that can be used. Person Search responses will include high-level person demographic information in addition to key application data such as Application ID and coverage year so that the EDE entity can determine whether an existing application should be

used for the consumer, or whether a new application needs to be created for the consumer. How to determine whether a new application needs to be created, or whether an existing application should be used, will be addressed in an upcoming [section](#).

The following are the current request options for the Person Search API. Data will be returned only if the searched consumer is on the latest version of an application.

- First Name
- Last Name
- Date of Birth
- Social Security Number (SSN)
- Zip
- City
- Coverage State
- Coverage Year
- Primary Contact Email

6.1.1 Agent/Broker (UI) Search vs. Consumer (Back-End) Search

The Person Search API can be leveraged as both a front-end (UI) and a back-end function. Agents/Brokers should be the only users that are able to leverage the Person Search API as a UI component. Agents/Brokers can collect the required demographic search parameters from the consumer and search for the consumer's corresponding application(s).

For the consumer flow, EDE Person Search should be used as a back-end service and EDE entities must not allow consumers to provide direct inputs into a Person Search UI component. EDE entities must use the demographic information collected during ID proofing to search for a consumer's application(s) in the EDE consumer flow. EDE entities will subsequently need to store the ID proofing data that is used to search for a consumer's application(s), for use in future interactions if the consumer returns to the EDE entity's site, given Person Search should always occur prior to any application update being initiated. Furthermore, EDE entities will need to capture updates to the ID proofing data, based on eligibility application interactions that result in changes to the previously provided ID proofing data. For example, if the ID proofed user reports a change in their legal name due to a marriage or divorce, the EDE entity would need to capture this name change in order to complete a successful search for the consumer's existing application(s) during future searches.

6.1.1.1 Agent/Broker Pathway Permission Attestation Requirement

EDE entities that provide an agent/broker pathway should note that they are required to include a permission attestation on the Person Search page that is exposed to agents/brokers in their UI. Agents/Brokers must be required to complete the permission attestation prior to completing a Person Search, and must receive an error if they attempt to search without completing the attestation. On HealthCare.gov, a checkbox is presented to agents/brokers that states, "Check here to indicate you've gotten permission from this person to search for his or her application." EDE entities do not need to implement the attestation exactly as it is on HealthCare.gov, but must provide a similar permission attestation in their agent/broker pathway.

6.2 Search Combinations

This section describes the minimum search criteria that EDE entities must use as part of the EDE Person Search API request. The minimum search criteria varies for the EDE consumer and EDE A/B flows. As such, the minimum search criteria for each flow is described separately below.

6.2.1 Minimum Search Criteria – EDE Consumer Flow

In the consumer flow, the EDE entity will complete a backend (i.e. not UI-facing) Person Search using the information obtained as part of the remote identity proofing process, to determine whether a consumer has any existing applications. There are two search options:

- 1) SSN + Date of Birth (DOB)
 - EDE entities are not required to use this search option, however CMS recommends this always be the first option when searching for a consumer's application.
 - If the SSN + DOB Search does not yield any results, or if an EDE entity does not utilize the SSN + DOB Search, then a demographic search must be used to determine whether a consumer has an existing application.
- 2) Demographic search with First Name + Last Name + DOB + either: 1) City or 2) Zip Code
 - CMS recommends that this be used as the second option when searching for a consumer's existing application.
 - If results are returned for multiple consumers using the demographic search, EDE entities can utilize one of two methods to identify the appropriate consumer application(s):
 - i. Add the Primary Contact Email to the search request (in addition to the above elements).
 - ii. Identify the appropriate application(s) by comparing the consumer's street address with those in the returned results

6.2.2 Minimum Search Criteria – EDE Agent/Broker Flow

In the agent/broker flow, the EDE entity can provide the agent/broker with a UI Person Search option. EDE entities can provide agents/brokers with the following two search options:

- 1) SSN + Date of Birth (DOB)
 - EDE entities are not required to provide this search option to agents/brokers, however CMS recommends this always be the first option when searching for a consumer's application.
 - If the SSN + DOB search does not yield any results (not all consumers provide SSNs), or the EDE entity does not implement the SSN + DOB search option, the EDE entity must require that agents/brokers use the demographic search option to determine whether a consumer has an existing application that can be updated.

2) Demographic search with First Name + Last Name + DOB

- EDE entities are required to provide this search option to agents/brokers.
- CMS recommends that this be used as the second option when searching for a consumer’s existing application.
- This search can be supplemented with:
 - i. City
 - ii. Zip Code
 - iii. Coverage Year
 - iv. Coverage State
 - v. Primary Contact Email


Below is an example of what the agent/broker Person Search might look like in an EDE entity’s UI:

To find a client’s existing application, enter his or her information.

SSN Search

Social Security Number (SSN)	Date of Birth	
<input type="text"/>	<input type="text"/>	
<small>XXX-XX-XXXX</small>	<small>MM/DD/YYYY</small>	<input type="button" value="SEARCH"/>

Demographic Search

First name	Coverage year	State
<input type="text"/>	<input type="text" value="Select..."/>	<input type="text" value="Select..."/>
Last name	Date of Birth	
<input type="text"/>	<input type="text"/>	
City	ZipCode	
<input type="text"/>	<input type="text"/>	
Email		<input type="button" value="SEARCH"/>
<input type="text"/>		

6.3 Search Results

The EDE Person Search API will only return a response if a record exactly matches the requested information. However, non-alphabetic characters will be ignored when matching first

name, last name, and city. For example, searching for “Mary Ann” may return “Mary-Ann” or “MaryAnn.” Similarly, searching for “St Louis” will match “St. Louis”, though it will not match “Saint Louis”. In addition, if the search includes coverage year as part of the demographic search option, the service will return the associated future year application if available. Associated future year applications will only be returned if the inputted coverage year is the current year. If the EDE Person Search user inputs a previous coverage year, then only the applications found in the inputted historical coverage year will be returned.

The Person Search service will return no more than 40 exact person matches to ensure a high level of confidence that the search results exactly match the requested criteria. If the EDE Person Search functionality finds 40 or more results, an error message will be returned asking the user to add additional search parameters. There is no ordering of search results in this functionality, results are returned in the order in which the records were found.

6.3.1 Person Search Response Data Elements

When the Person Search query results in an exact match for the information provided in the request, the Person Search response will return demographic and application-related data associated with any matches. Below are the potential data elements that will be returned in the Person Search response, although the exact set of data returned in each response will vary:

- Person Tracking Number (PTN)
- First Name
- Last Name
- Date of Birth
- SSN
- Email Address
- Street Address 1
- Street Address 2
- City
- State
- Zip Code
- Application ID
- Latest Application Version
- Latest Application Version Consumer is On
- Coverage Year
- Coverage State
- Primary Email
- Primary Telephone
- Secondary Telephone
- Additional PTN Indicator (whether there are additional PTNs tied to the application)
- Application Status
- Application Last Modified Date/Time
- Additional Policy Indicator (whether there are additional policies tied to the application)

-
- Marketplace Group Policy Identifier (policies tied to the person)
 - Subscriber Indicator

EDE entities should view the EDE Person Search API Specs available via zONE (<https://zone.cms.gov/document/enhanced-direct-enrollment-edo-documents-and-materials>) for the detailed response specifications.

6.4 Determining Whether a New Application Needs to Be Created or Whether an Existing Application Should Be Used

When the Person Search query results in an exact match for the information provided in the request, the Person Search response will include demographic and application-related data that will be used by the EDE entity (and/or agent/broker) to determine whether a new application needs to be created for the consumer, or whether an existing application can be used. This section describes the criteria that EDE entities must consider when making this determination.

6.4.1 When to Use an Existing Application

When the Person Search query results in an exact match for the information provided in the request, and the EDE entity (or agent/broker) determines the information is for the applicable consumer, the EDE entity (or agent/broker) must use an existing application that is returned under any of the following circumstances:

- 1) The application returned is for the correct coverage state and coverage year that the consumer is applying for.
 - In this instance, the EDE entity (or agent/broker) can “claim” the application and use the applicable Application ID in subsequent API calls to request permission and update the existing application.
- 2) The application returned is for the correct coverage state that the consumer is applying for, but is for the prior coverage year (i.e. coverage year the consumer is applying for, minus one year), and the application is not a version 1 application that is in an in-progress state.
 - In this instance, the EDE entity (or agent/broker) will use this Application ID to prepopulate an application for the requested coverage year via the Create App from Prior Year App API.

6.4.1.1 Determining Which Application to Use When There are Multiple Applications for a Specific Coverage Year and Coverage State

While the FFM generally tries to prevent consumers from having duplicate applications, there will be instances where the Person Search API returns multiple applications for a consumer for a specific coverage year and coverage state. When multiple applications are returned for a consumer for a specific coverage year and coverage state, EDE entities (or agents/brokers) will need to determine which application to use if the existing application should be updated, or if the existing application should be used to prepopulate an application for the coverage year that the consumer is applying for. To make this determination, EDE entities will use the Application

Status (applicationProcessStatus) and Application Last Modified Date/Time (applicationLastModifiedDateTime) returned in the Person Search, as described below:

- 1) If the Person Search yields one or more COMPLETE_ENROLLED application for a consumer for a specific coverage year and coverage state, only these applications should be used.
 - EDE entities are permitted to allow the agent/broker or consumer to select the COMPLETE_ENROLLED application they want to use in this instance.
- 2) If the Person Search does not yield any COMPLETE_ENROLLED applications, but does return multiple SUBMITTED_ENROLLMENT_PENDING applications for a consumer for a specific coverage year and coverage state, only these applications should be used.
 - EDE entities are permitted to allow the agent/broker or consumer to select the SUBMITTED_ENROLLMENT_PENDING application they want to use in this instance.
- 3) If the Person Search does not yield any COMPLETE_ENROLLED or SUBMITTED_ENROLLMENT_PENDING applications for a consumer, but does return multiple of any of the following for a specific coverage year and coverage state, then only the last modified of these applications should be used:
 - SUBMITTED_NO_ENROLLMENT
 - SUBMITTED_ENROLLMENT_TERM_CANCEL
 - COMPLETE_NO_QHP_ELIGIBILITY
 - COMPLETE_LIMITED_PLAN_AVAILABILITY
- 4) If the Person Search only yields IN_PROGRESS applications for a consumer for a specific coverage year and coverage state, then the last modified of these applications should be used.

6.4.2 When to Create a New Application

When the Person Search query results in an exact match for the information provided in the request, and the EDE entity (or agent/broker) determines the information is for the applicable consumer, the EDE entity (or agent/broker) will need to determine whether the existing application can be used as described in the above section. However, there will be instances when a new application needs to be created for a consumer. Below are the instances when it is appropriate for an EDE entity (or agent/broker) to create a new application via the Create App API:

- 1) The Person Search query does not return any matching results for the information provided in the request.
- 2) The application returned is for the correct coverage year that the consumer is applying for, but the application is not for the correct coverage state.
- 3) The application returned is for the prior coverage year (i.e. coverage year the consumer is applying for, minus one year), but the application is not for the correct coverage state.

-
- 4) The application returned is for the correct coverage state, however it is for a coverage year that is two or more years prior to the coverage year that the consumer is currently requesting coverage for.
 - 5) The application returned is for the correct coverage state that the consumer is applying for, but is for the prior coverage year (i.e. coverage year the consumer is applying for, minus one year), and the application is version 1 and is in an “in-progress” state.
 - Note, if a prior coverage year application is returned with the correct coverage state, and it is version 2 or greater, then EDE entities (or agents/brokers) are still required to repopulate an application from the prior year application using the Create App from Prior Year App API, even if the most recent version is in an “in-progress” state.
 - When sending the request to the Create App from Prior Year App API in this scenario, EDE entities will need to either: 1) send the request without an application version number, or 2) send the request with the application version that is in a “complete” or “submitted” state.

7 Notice Retrieval

7.1 Notice Retrieval Overview

The EDE Notice Retrieval API will enable consumers and agent/brokers to download and view Marketplace notices through an EDE entity website. As a requirement, EDE entities should not internally store Marketplace generated notices but should retrieve them from the Marketplace based on a consumer or agent/broker initiated UI request.

To display a notice, EDE entities will need to make two separate API calls - the first to the Metadata Search API and the second to EDE Notice Retrieval API.

7.2 Searching for Metadata Record – Retrieving DSRS ID

The Metadata Search API enables EDE entities to search for and retrieve the DSRS Identifier (DSRS ID) along with other metadata tied to a document.

EDE entities will provide an Insurance Application Identifier as the request parameter for Metadata Search to retrieve DSRS IDs tied to Marketplace documents. If the requesting EDE entity has permission to work on the associated application, the Metadata Search API will return all metadata records tied to the application. Metadata records that may be returned include Marketplace notices and consumer supporting documentation uploaded through EDE websites. Metadata records for Marketplace notices will be indicated by a Document Category equal to “NOTICE,” while metadata records for consumer uploaded supporting documentation will have Document Category equal to “SUPPORTING_DOC.”

Metadata Search also provides the capability to filter search results by various metadata attributes. For instance, if an EDE entity wishes to only retrieve metadata tied to notices, documentCategoryCode “NOTICE” can be added into the search request along with the

Insurance Application Identifier. This will ensure that Metadata Search only returns records tied to notices

Please note that Marketplace notices will only be tied to the application version the notice was initially generated for. If the notice is carried over to a subsequent version of an application, this subsequent version will not be reflected in DSRS metadata. Therefore, if an EDE entity chooses to filter Metadata Search Results by Application Version Number, only the initial version the notice was generated for should be utilized.

Each notice Metadata record returned will include the DSRS ID of the associated notice along with the following attributes:

Table 7-1: Notice Metadata

Metadata Attribute	Description
documentCategoryCode	This provides a high-level description of the type of document.
sourceSystemCode	This describes the system submitting the document and corresponding metadata. Certain document categories can be submitted by multiple source systems. Source system will provide insight into what system the document originated from or was submitted to (by a consumer) and can be useful when resolving consumer issues.
fileFormat	File format designates the format of the file in DSRS.
fileSize	Size of the document in bytes.
documentCreationDateTime	DateTime the document was created by the source system.
documentFileName	Name of the file with the extension. For notices, this will be the file name given to the physical document by the source system.
documentSubcategoryCode	Document subcategory offers a more detailed description of the document within a specific document category. Subcategory is one of the factors for authorization. Examples: Eligibility Result Notice, Form 1095A
insuranceApplicationIdentifier	Unique identifier tied to an insurance application.
applicationVersionNumber	Version of the application that a notice is being sent for.
coverageYear	Year during which consumer receives benefits coverage. Notices are only tied to one coverage year.
personTrackingNumbers	Unique tracking number for the person within the Marketplace.
marketplaceGroupPolicyIdentifier	Unique identifier of an insurance application.
exemptionApplicationIdentifier	Identifier tied to an exemption notice.
applicationMemberIdentifier	A unique system generated number used to identify an Application Member.
consumerAttestedDocumentType	Type of supporting document the consumer attested to uploading.
eswDeterminedDocumentType	Type of supporting document as determined by the Eligibility Support worker.
restrictedResultIndicator	Boolean indicating whether search results were hidden due to client system authorizations

7.3 Retrieving Notices

The DSRS ID provided in each Metadata record can be used in the Notice Retrieval API to retrieve the notice itself. EDE entities will provide the DSRS ID associated to the notice they would like to display in the request URI. If the EDE entity has permission to work on the application tied to the notice, the Notice Retrieval API will return a time-expiring link. The URL will expire after 30 seconds. The EDE entity will auto-redirect to the link provided in the response in order to trigger the download.

7.4 Form 1095-A Overview

Form 1095-A is a prepopulated tax form similar to a Form W-2, sent to individuals who enrolled themselves, or one or more of their tax household members, in a qualified health plan (QHP) through the FFM. Form 1095-A provides consumers with information about their health coverage needed to file their taxes, reconcile advance payments of the premium tax credit (APTC), and claim the premium tax credit (PTC). Consumers ultimately need the information on Form 1095-A to complete Form 8962. Consumers must complete Form 8962 and file it with their tax return if they want to claim the PTC or if they received premium assistance through APTC (whether or not consumers otherwise are required to file a tax return).

By January 31st each year, the CMS generates initial Forms 1095-A for the prior plan year and sends them to consumers. Beginning each February, if updates are made to enrollment data that appears on Forms 1095-A, CMS will generate a corrected or voided Forms 1095-A, and send them to consumers. Below are the types of Forms 1095-A consumers may receive:

- Initial Form 1095-A: The initial/original versions of Form 1095-A created for that plan year, which precede all subsequent versions of the form.
- Corrected Form 1095-A: Updated versions of Form 1095-A, which are sent to members if there are errors on the initial Form 1095-A.
- Void Form 1095-A: Updated versions of Form 1095-A, which are sent to members if the policy associated with the Form 1095-A is cancelled.

EDE entities may receive a number of questions from consumers related to Form 1095-A. Below are some of the questions EDE entities may receive, and where the questions should be routed.

- Questions that should be directed to the Marketplace:
 - 1) Why did I receive this Form 1095-A?
 - 2) Where can I find 2014, 2015, and 2016 Forms 1095-A in my online account?
 - 3) How do I get another mailed copy of my Form 1095-A?
 - 4) What do I need to do with this Form 1095-A?
 - 5) What does this information on the Form 1095-A mean?
 - 6) Why did I get more than one Form 1095-A?
 - 7) This information does not look correct. How can I change it?
 - 8) I added a dependent, but they are not on my Form 1095-A. What should I do?
- Questions that Should be Directed to the IRS:

-
- 1) Do I qualify for PTC?
 - 2) Do I owe an individual shared responsibility payment?
 - 3) What are the requirements for the individual shared responsibility provision?
 - 4) How do I report health care coverage on my income tax return?
 - 5) Will IRS verify that consumers had minimum essential coverage (MEC)?
 - 6) I received a Form 1095-A. How should I report this on my income tax return?
 - 7) Can you help me complete my income tax return?
 - 8) How do I use the Form 1095-A to fill out my Form 8962?
 - 9) Can I get a copy of the Form 8965 or 8962?
 - 10) I received a corrected Form 1095-A. Do I need to amend my income tax return?
 - 11) What happens if I don't file my income tax return?
 - 12) I can't file/can't pay my tax liabilities by April 15th. What should I do?

7.4.1 Retrieving and Displaying Form 1095-A

EDE entities must only retrieve and display initial, corrected, and voided Forms 1095-A for consumers that are for plan year (PY) 2017 and beyond. EDE entities must not retrieve and display initial, correct, and voided Forms 1095-A for consumers that are for PY2016 and earlier. Consumers receive both manually generated and automatically generated Forms 1095-A. However, manual Forms 1095-A are not available via the Notice Retrieval API for PY2016 and earlier. If an EDE entity displays a Form 1095-A that is for PY2016 or earlier, the Form 1095-A may be inaccurate, as it may not be the most recent manually generated Form 1095-A for the consumer.

7.4.2 Form 1095-A Notice Retrieval Testing

EDE entities do not have the ability to generate a Form 1095-A in the testing environment. CMS however does have the ability to generate these forms in the testing environment. Therefore, if an EDE entity wishes to test retrieving a Form 1095-A in the testing environment, the EDE entity can request applications that can be used to test this functionality. EDE entities that wish to request applications to test this functionality should send an email to Joshua.Halsey@cms.hhs.gov with the subject line, "Request for Applications to Test 1095-A Notice Retrieval". Upon request, the EDE entity will be provided with applications that have an Initial, Void, and Corrected Form 1095-A available for retrieval.

8 Document Upload

8.1 Document Upload Overview

The EDE Document Upload API will enable consumers and agents/brokers to upload supporting documentation intended for Data Matching Issue (DMI) or Special Enrollment Period (SEP) Verification Issue (SVI) adjudication through an EDE entity website. The EDE Document Upload API will be utilized to prevent the need for a redirect to myAccount on healthcare.gov.

8.2 Uploading a Document

To upload a document into the system, EDE entities must provide the file attachment along with corresponding metadata. Metadata includes data about the document such as document properties as well as document-category specific business and consumer information. Upon upload of a document, an EDE entity will be required to provide the following information that will be stored as metadata associated to the file:

- Document Category
- Source System
- File Size
- Document Creation Date Time
- Document File Name
- File Format
- Consumer Attested Document Type
- Person Tracking Number(s)
- Insurance Application Identifier
- Submission Method
- Issue Type
- Consumer Attested Verification Issue Identifier

A successful upload into the system will return a DSRS Identifier, a unique identifier tied to every document stored in the system.

8.3 Providing Document Feedback to Consumer

EDE entities can present feedback to consumers related to uploaded documents in their User Interface (UI) using the DSRS Metadata Search API. Metadata Search provides the capability to retrieve metadata associated to documents, as described in the previous [section](#).

9 Get Enrollment

9.1 Get Enrollment Overview

The Get Enrollment API allows EDE entities to retrieve enrollment data for a consumer. This service will allow users to view Insurance Plan Policies (IPPs) and Pended Plan Selections (PPSs) on the EDE entity's site, aligning with the overall goals of EDE. EDE entities will be able to retrieve a consumer's enrollment data by sending a request with an Insurance Application Identifier. The Get Enrollment API will return all enrollment data tied to an application that the requester has been authorized and received permission to view. EDE entities will be able to request enrollment data for consumers once an IPP or PPS has been created.

There are two types of entities that can make a request to the Get Enrollment service -- an issuer and a web-broker. EDE entities must indicate if they are an issuer or a web-broker when onboarding with the Hub. The Hub will then share this information with the FFM for each request sent to the Get Enrollment API. Once the request is sent, the API will check if the

requesting entity has “permission” to view the policies tied to the application that they are requesting by sending the Application ID and the Partner ID to the Permission API. Access to Get Enrollment data will be granted as follows based on partner type and permission:

Table 9-1 - Get Enrollment Permission Matrix

Partner-Type	Permission	No Permission
Issuer	<p>For all policies on an application with a HIOS ID tied to the issuer, allow the issuer to view any:</p> <ul style="list-style-type: none"> • IPPs • PPSs <p>For all policies on an application with a HIOS ID tied to a different issuer:</p> <ul style="list-style-type: none"> • Limited Enrollment Response 	<p>For all policies on an application with a HIOS ID tied to issuer, allow the issuer to view any:</p> <ul style="list-style-type: none"> • IPPs
Web-Broker	<p>For all policies on an application, allow the web-broker to view any:</p> <ul style="list-style-type: none"> • IPPs • PPSs 	Error message will be returned.

9.1.1 UI Display of Get Enrollment Data

EDE entities are required to make enrollment data available in their UI, in both the consumer and agent/broker flows. At minimum, EDE entities should display the same enrollment data that would be available to a consumer or agent/broker on HealthCare.gov. The minimum data that must be displayed in the UI is described below:

- EDE entities must display all of a consumer’s active policies. EDE entities may choose to display active policies in one of two ways:
 - EDE entities may choose to display a policy as active until: 1) cancellation of the policy occurs, or **2) termination of the policy occurs and the current date is beyond the termination date of the policy.** If using this display method, an active policy will have an insurancePolicyStatusType of ACTIVE_OR_TERMINATED, and an insurancePolicyEndDate that is the current date or a future date.
 - EDE entities may choose to display a policy as active until: 1) cancellation of the policy occurs, or **2) termination of the policy occurs.** If using this display method, an active policy will have an insurancePolicyStatusType of ACTIVE_OR_TERMINATED, and an insurancePolicyEndDate that: 1) equals

12/31 of the respective coverage year, and 2) has a specifiedEoyEndDateIndicator of false.

- EDE entities must display all of a consumer’s terminated policies. EDE entities may choose to display terminated policies in one of two ways:
 - EDE entities may choose to display a policy as terminated only after the actual termination date of the policy. If using this display method, a terminated policy will have an insurancePolicyStatusType of ACTIVE_OR_TERMINATED, and an insurancePolicyEndDate that is prior to the current date.
 - EDE entities may choose to display a policy as terminated as soon as termination occurs, regardless of the termination date. If using this display method, a terminated policy will have an insurancePolicyStatusType of ACTIVE_OR_TERMINATED, and an insurancePolicyEndDate that either: 1) does not equal 12/31 of the respective coverage year, or 2) equals 12/31 of the respective coverage year but the specifiedEoyEndDateIndicator is true.
- EDE entities must display all of a consumer’s cancelled policies and all of a consumer’s Pended Plan Selections that have been cancelled.
 - A cancelled policy will have an insurancePolicyStatusType of CANCELLED.
 - A Pended Plan Selection that is cancelled will have an insurancePolicyStatusType of PEND, and a statusType (pendedPlanSelectionSummary.currentStatus.statusType) of PEND_CANCELED.
- EDE entities must display all of a consumer’s Pended Plan Selections.
 - A Pended Plan Selection will have an insurancePolicyStatusType of PEND, and a statusType (pendedPlanSelectionSummary.currentStatus.statusType) of PEND.
 - Note, Pended Plan Selections with a statusType (pendedPlanSelectionSummary.currentStatus.statusType) of PEND_RELEASED, do not need to be displayed in the UI. When a Pended Plan Selection is released, a policy is created, and therefore the EDE entity will only display the associated policy.
- EDE entities must also display the following data associated with the policy or Pended Plan Selection:
 - QHP ID
 - selectedInsurancePlan
 - Plan Name
 - The plan name can be obtained from the Public Use Files (PUFs), the Marketplace API, etc.
 - Start Date
 - insurancePolicyStartDate
 - End Date
 - insurancePolicyEndDate

-
- Total Premium
 - `insurancePolicyPremium.monthlyPolicyPremiumAmount`
 - Applied APTC
 - `insurancePolicyPremium.appliedAptcAmount`
 - Individual Responsibility Amount
 - `insurancePolicyPremium.individualResponsibleAmount`
 - Enrollees
 - `coveredInsuredMembers.memberInformation.firstName`
 - `coveredInsuredMembers.memberInformation.middleName`
 - `coveredInsuredMembers.memberInformation.lastName`
 - `coveredInsuredMembers.memberInformation.suffixName`

When multiple policies or Pended Plan Selections are returned in the Get Enrollment response, EDE entities should always display the policy or Pended Plan Selection with the latest `insurancePolicyStartDate` first, followed by the policy or Pended Selection with the next latest `insurancePolicyStartDate`, and so on and so forth. If multiple policies or Pended Plan Selections are returned with the same `insurancePolicyStartDate`, EDE entities should display any that are active or pended first, followed by any that are cancelled or terminated. For example, if the Get Enrollment response includes two policies, one with an 8/1/2019 `insurancePolicyStartDate` and one with a 1/1/2019 `insurancePolicyStartDate`, the EDE entity should prioritize the display of the policy with the 8/1/2019 `insurancePolicyStartDate`. Or for example, if the Get Enrollment response includes two policies with a 1/1/2019 `insurancePolicyStartDate`, and one policy is active and one is cancelled, the EDE entity should prioritize the display of the active policy.

Issuer EDE entities should also be aware that they may receive a Limited Enrollment Response when a consumer is enrolled with a different issuer. In this instance, EDE entities are permitted to display more limited enrollment information to the consumer, based on what is available in the Limited Enrollment Response.

Below is an example of an active policy displayed in the HealthCare.gov UI:

Status: Initial Enrollment

**MyPriority HMO
Silver 3200
29698MI0540150**

VIEW PLAN BENEFITS

Base premium **\$917.48/mo.**
[Premium tax credit](#) **\$-570.15/mo.**

You pay: **\$347.33/mo.**

Members:	Start date:	End date:	Action:
Dad Michigan	09/01/2019	12/31/2019	REMOVE

Coverage record

Coverage dates	Premium	Premium tax credit	You pay	Members
09/01/2019 - 12/31/2019	\$917.48	\$570.15	\$347.33	Dad

You can view the personal information, like your name and address, that we sent to your plan.

VIEW MY PLAN PROFILE

You can only change plans during Open Enrollment for 2019 or if you're eligible for a Special Enrollment Period.

CHANGE PLANS

9.1.2 EDE Issuers – Using Get Enrollment as a Standalone Tool

EDE issuers, please note that CMS will permit the use of Get Enrollment as a standalone tool, outside of the standard EDE consumer and agent/broker flows. For example, EDE issuers may want to make a Get Enrollment UI available to their call center representatives, which can be

used to look up a consumer's enrollment data. Note that the use of Get Enrollment in this fashion, is not permitted for EDE web-brokers.

A Get Enrollment UI can be made available to both agent/broker and non-agent/broker issuer employees. Note that the same EDE ID proofing requirements that apply to EDE agents/brokers would apply to agent/broker and non-agent/broker issuer employees that are using Get Enrollment as a standalone service. Specifically, all issuer employees using Get Enrollment as a standalone service will either need to be manually or remotely identity proofed. Manually ID proofing can be completed as described in the "Acceptable Documentation for ID Proofing" document on the EDE page on zONE at <https://zone.cms.gov/document/enhanced-direct-enrollment-edo-documents-and-materials>. Remote ID proofing can be completed using the RIDP/FARS services. If employees have already been ID proofed as part of standard employment processes, no additional ID proofing needs to occur.

In addition to the ID proofing requirements for issuer employees, EDE issuers must also abide by the following requirements if using Get Enrollment as a standalone tool:

- The Get Enrollment UI will need to be maintained within the EDE entity's security perimeter.
- The use of Get Enrollment as a standalone tool will need to be included as part of the EDE entity's privacy and security audit.
 - Alternatively, post-audit submission, EDE entities intending to use Get Enrollment as a standalone tool can submit an EDE entity-initiated change request, as described in the Third-party Auditor Operational Readiness Reviews for the Enhanced Direct Enrollment Pathway and Related Oversight Requirements available on zONE at <https://zone.cms.gov/system/files/documents/guidelines-for-third-party-auditors-edo-py19py20.pdf>.
- When submitting transactions via the Get Enrollment API:
 - The Role-Id submitted in the header of the API request will be "ISSUER".
 - The User-Id submitted in the header of the API request will be either the User ID for the individual user in the issuer's system, or some unique identifier for the individual user.
- Issuers must not run any batch processes through the Get Enrollment API.

Note also, in order for an issuer to use Get Enrollment as a standalone service, the appropriate insurance company relationship(s) will need to be set up in HIOS. If instructions for setting up the appropriate relationships are needed, please send an email requesting instructions to cms_feps@cms.hhs.gov, CMS.FFM.EDESupport@accenturefederal.com, and Hubsupport@sparksoftcorp.com.

10 DMI

10.1 DMI Overview

The DMI API allows EDE entities to access data related to Data Matching Issues (DMIs) that a consumer may have. The API will retrieve data from both the FFM database, as well as the ESW Clearinghouse database, in order to provide EDE entities with maximum information related to any DMIs that a consumer may have.

When assisting consumers with DMIs, EDE entities will need to inform consumers what documentation is required to resolve the DMIs, and also allow consumers to upload documentation to resolve the DMIs. The following link can be used as a reference to identify which documents are required to resolve specific DMIs: <https://www.healthcare.gov/verify-information/documents-and-deadlines/>.

EDE entities can retrieve data from the DMI API by submitting a request to the API with the applicable Insurance Application Identifier. EDE entities must also have been granted permission by the consumer in order to retrieve DMI data. Requests may only include one Application Identifier at a time and responses for a request will include all members associated with that application.

Since the DMI API pulls both FFM and ESW data, and some of that data overlaps, certain data elements should be considered as the source of truth. FFM DMI data will provide the ultimate status of the DMI, while the ESW data will provide the intermediate status and additional status details that are a part of ESW's task workflow. Each source provides application, DMI, and person data (ESW DMI service only provides PTN for person data). In conjunction, FFM plus ESW data is meant to provide a holistic view of a consumer's DMI status. FFM data is the source of truth for the final eligibility disposition on the consumer's DMI status. Refer to the below "Table 10-1 - Overlapping DMI Fields" to determine which systems are the source of truth when there is an overlap between fields.

Table 10-1 - Overlapping DMI Fields

DMI Field Name	Source of Truth	Description
DMI Type	FFM	FFM's 'verificationType'/'dmiSubType' and the 'dmiType'/'dmiSubType' ESW fields are duplicative in the DMI API response. These fields will usually match, but there are some instances that result from application versioning/soft-delete scenarios, where these fields may not match between FFM and ESW data sources.
DMI Status	FFM	The FFM field 'dmiStatus' and ESW field 'eswDmiStatus' may not always match. The FFM is the source of truth

DMI Field Name	Source of Truth	Description
		for the overall disposition, meaning the FFM dmiStatus will provide the final disposition of a DMI, while the eswDmiStatus will provide interim statuses as the verification tasks are underway.
DMI Expiration Time Clock	FFM	Both the FFM and ESW responses will contain a timer indicating the period in which a consumer must provide supporting documentation to resolve their DMI. The timer end date that should be used should be from the FFM response.

10.2 Consolidated Status

The DMI API will also provide a field in the FFM response called consolidatedDmiStatus. This field takes the status from the FFM and ESW as an input and provides a consumer friendly value indicating the overall status of the DMI. It is recommended that EDE entities use the consolidatedDmiStatus to convey the status of the DMI to the consumer.

11 SVI

11.1 SVI Overview

The SVI API allows EDE entities to access data related to Special Enrollment Period (SEP) Verification Issues (SVIs). The API will retrieve data from both the FFM database as well as the ESW Clearinghouse, in order to provide EDE entities with maximum information related to any SVIs that a consumer may have.

When assisting consumers with SVIs, EDE entities will need to inform consumers what documentation is required to resolve the SVIs, and also allow consumers to upload documentation to resolve the SVIs. The following link can be used as a reference to identify which documents are required to resolve specific SVIs: <https://www.healthcare.gov/coverage-outside-open-enrollment/confirm-special-enrollment-period/>.

EDE entities can retrieve data from the SVI API by submitting a request to the API with the applicable Insurance Application Identifier. EDE entities must also have been granted permission by the consumer in order to retrieve SVI data. Requests may only include one Application Identifier at a time and responses for a request will include all members associated with that application.

Similar to the DMI API, the SVI API also pulls data from two data sources: the FFM and ESW. Similarly, the two data sources will return some overlapping information. The FFM SVI data

will provide the ultimate status of the SVI, while the ESW data will provide the intermediate status and additional status details that are part of the ESW’s task workflow. FFM plus ESW data is meant to provide a holistic view of a consumer’s SVI status. Refer to the below “Table 11-1 - Overlapping SVI Fields” to determine which systems are the source of truth when there is an overlap between fields.

Table 11-1 - Overlapping SVI Fields

SVI Field Name	Source of Truth	Description
SVI Type	FFM	FFM’s verificationStatusReason and the sviType ESW field are duplicative and return similar information. These fields will usually match, but there are cases due to technical errors where these fields may not match between the FFM and ESW.
SVI Status	FFM	The FFM field ‘timerStatusType’ and ESW’s ‘eswSviStatus’ may not always match. The FFM is the source of truth for the overall disposition meaning that the FFM timerStatusType will provide the final status of a SVI, while the eswSviStatus will provide interim statuses as the SVI is being adjudicated.
SVI Expiration Time Clock	FFM	Both the FFM and ESW response will contain a timer indicating the period in which a consumer must provide supporting documentation to resolve their SVI. The timer end date that should be used should be taken from the FFM response.

11.2 Consolidated Status

The SVI API will also provide a field in the FFM response called consolidatedSviStatus. This field will take inputs from the timerStatusType field in FFM and the sviDisposition and sviReason fields in ESW and merge them into a consumer-friendly disposition. It is recommended that EDE entities use the consolidatedSviStatus to convey the status of the SVI to the consumer.

12 Standalone Eligibility Services (SES)

12.1 SES Overview

The SES APIs allow EDE entities to create, update, submit, delete, and retrieve application data. These APIs will be an integral component of an EDE build, as these APIs will be used to build the eligibility application for the EDE entity's platform. While some information related to the SES APIs is included in the various sections within this document, EDE entities will find the vast majority of information necessary for integrating with the SES APIs and building the eligibility application on zONE at <https://zone.cms.gov/document/enhanced-direct-enrollment-edo-documents-and-materials>. In particular, EDE entities will rely heavily on the below documents when integrating with the SES APIs and building the eligibility application, however there is a plethora of useful material available on zONE, and EDE entities should be sure review all of the information available.

- UI Question Companion Guide - This document outlines the UI requirements that must be met in order to successfully integrate an eligibility application with the SES API suite.
- FFE UI Application Principles for Integration with FFE APIs - This document outlines the guiding principles of a user-interface (UI) application or system and its integration with the FFE APIs for eligibility services. This document covers both technical and policy requirements for integrating with the FFE APIs.
- FFE UI Application Services for Eligibility Services: General and Technical FAQs - Expands on the other documentation for the FFE APIs by capturing frequently asked questions and lessons learned on how external user interfaces (UIs) should interact with the FFE's eligibility APIs.
- EDE API Specs - This zip file contains the current API Specs for the EDE APIs.

12.2 Health Coverage Verification

The Health Coverage Verification (HCV) service provides real-time verification for consumers who attest to losing Minimum Essential Coverage (MEC) through a non-Exchange healthcare plan. This verification may allow consumers who are eligible for a Special Enrollment Period (SEP), due to the loss of MEC, to enroll in a healthcare plan without creating a SEP Verification Issue (SVI), which would require manual verification of documentation provided by the consumer. Health Coverage Verification is accomplished by calling a Trusted Data Source (TDS) prior to application submission, where the TDS may or may not be able to confirm that the consumer lost MEC. When the TDS is able to confirm that the consumer lost MEC, this leads to an improved consumer experience and a decreased workload Eligibility Support Workers (ESWs).

While EDE entities will not interact with the HCV service directly, certain fields must be provided by EDE entities via the Update App API, prior to the HCV call being made. As the HCV call can take up to one minute to process, CMS recommends that EDE entities provide the necessary information via the Update App API as soon as the necessary data is provided by the consumer.

To ensure that HCV can be completed prior to application submission, and ensure the best possible consumer experience, EDE entities must do the following:

- 1) Collect the Loss of MEC Attestation early enough in the EDE UI flow, such that the HCV response will be present at application submission (up to 1 minute later).
- 2) Make a subsequent Update App call as soon as the following data is collected for the consumer:
 - a) Name: First Name, Last Name, Middle Name (Optional), Suffix (Optional)
 - b) Address: Street Name 1, Street Name 2 (Optional), City, State, Zip Code, Plus 4 Code (Optional)
 - c) Gender
 - d) Date of Birth
 - e) Email Address
 - f) SSN (Optional)
 - g) Loss of MEC Attestation

While the HCV call is made after the necessary information is provided to the Update App API, the logic for the Loss of MEC SEP verification will be run after the Submit App API request. If a consumer is eligible to enroll and the Loss of MEC is verified by HCV, an SVI will not be generated and the consumer will be free to enroll after application submission. An SVI will be generated for consumers who are eligible, but where the Loss of MEC is unable to be verified by HCV. Consumers that receive an SVI will have to manually verify their eligibility for the SEP, prior to any Pended Plan Selection (PPS) being sent to the issuer.

12.3 Optimistic Locking

EDE entities integrating with the SES APIs should be aware that the majority of the SES APIs use optimistic locking, whereby when one SES API request is submitted, a subsequent SES API request cannot be submitted until the prior request has been processed. Accordingly, EDE entities should be mindful of optimistic locking when integrating with the SES APIs, particularly when integrating with the Update App, Add Member, Remove Member, and Submit App APIs. EDE entities must ensure that they integrate with these APIs in a way that prevents subsequent API requests from being submitted, prior to receiving a response for a previous API request. For example, EDE entities will need to make several Update App requests as a user progresses through the eligibility application, however a user should not be able to initiate an action in the UI that results in an Update App request being sent prior to a previous Update App response being returned. In the event that an EDE entity doesn't appropriately prevent SES API requests from being triggered prior to a previous SES API response being returned, the subsequent API requests will fail and return an `OPTIMISTIC_LOCKING_ERROR` in the response.

13 Payment Redirect

13.1 Payment Redirect Overview

When a consumer initially enrolls in coverage, or when a consumer switches plans, the consumer will need to make a binder payment in order to effectuate their coverage. The EDE Payment Redirect API gives EDE entities the ability to redirect eligible consumers to issuer websites to make their binder payments.

When an EDE entity submits a request to the Payment Redirect API, the FFM will first verify that the EDE entity has permission to work on the consumer's behalf. If permission is verified, the FFM will then verify whether the consumer is eligible for payment redirect. If the consumer is eligible for payment redirect, the Payment Redirect API response will indicate this eligibility, and will also include the URL for the issuer's payment portal, along with Security Assertion Markup Language (SAML) that can be posted to the issuer's payment portal, allowing the consumer to make their binder payment.

Consumers are generally eligible to be redirected to make a binder payment using the Payment Redirect API if all of the following conditions are met:

- 1) The issuer has provided the FFM with their payment portal information.
- 2) The consumer's policy is active and has not already been effectuated.
 - Note, if the consumer receives a Pended Plan Selection (PPS) due to a SEP Verification Issue (SVI), the consumer will not be eligible for payment redirect until the SVI has been resolved and the PPS has been released to the issuer.
- 3) The consumer's coverage effective date is in the future.
 - Note, after the effective date of the policy, the consumer will not be eligible for payment redirect. So for example, if a new policy is created with a newborn SEP, and the effective date is retroactive, the consumer will not be eligible for payment redirect.
- 4) For dental plans only, a consumer will only be able to complete the payment redirect if the dental policy has a guaranteed premium.
 - To be clear, if a dental policy has an estimated premium, the consumer will not be eligible for payment redirect.

13.2 Payment Redirect Response

The EDE Payment Redirect API will return any applicable consumer policy information for each policy tied to the Insurance Application Identifier provided in the request. So for example, if there are both health and dental policies tied to an application, the Payment Redirect response may include two separate sets of policy information. The API response will return the below information for each policy when applicable:

- Payment Redirect Eligible Indicator

-
- Payment Redirect SAML
 - Exchange Assigned Policy Identifier
 - Issuer Payment Website URL

For applications with multiple policies, EDE entities should redirect each policy individually. For example, if an application has both a health policy and a dental policy tied to it, the EDE entity will post two separate SAMLs to the each of the respective issuer payment portals, in order for each binder payment to be made.

EDE entities will know whether a consumer is eligible for payment redirect by checking the Payment Redirect Eligible Indicator and Issuer Payment Website URL in the Payment Redirect API response. When the Payment Redirect Eligible Indicator is set to true, and the issuer has provided an Issuer Payment Website URL, the consumer is eligible to redirect and make a binder payment for their policy. If the Payment Redirect Eligible Indicator is set to false, or if there is no Issuer Payment Website URL, then the consumer is ineligible to redirect to make the binder payment for their policy.

The Payment Redirect SAML is built from FFM policy information, and includes the same information that is sent for a consumer completing payment redirect directly via healthcare.gov. EDE entities must not alter the SAML information. If the private/public key signature is invalidated, the issuer should reject the request for payment redirect.

13.3 Payment Redirect Integration Requirements

EDE entities are required to integrate with the Payment Redirect API, and must provide consumers that are eligible for payment redirect with a UI option that allows them to be redirected to their issuer's payment portal to make a binder payment. The one exception to this requirement is for EDE entities that have implemented their own binder payment functionality. For example, an issuer EDE entity may have their own payment portal, and may provide a UI option in their EDE pathway that allows all eligible consumers to navigate directly to the payment portal to make a binder payment. Or for example, a web-broker EDE entity may have their own payment redirect functionality established directly with all of the issuers in the states they work in, and may provide a UI option in their EDE pathway that allows all eligible consumers to be redirected to their respective issuers for binder payments when applicable. If an EDE entity has their own binder payment functionality established that meets the following requirements, no integration with the Payment Redirect API is required:

- 1) The EDE entity's binder payment functionality must allow all eligible consumers to make binder payments to their respective issuers.
 - a. To be clear, if an EDE entity supports enrollment for multiple issuers, the EDE entity's binder payment functionality must allow a binder payment to be made to each of the respective issuers, when a consumer is eligible to make a binder payment with any of the respective issuers.
 - b. The EDE entity's UI must allow eligible consumers to make a binder payment when the following apply:
 - i. The consumer's policy is active and has not already been effectuated.

-
1. Note, if the consumer receives a Pended Plan Selection (PPS) due to a SEP Verification Issue (SVI), the EDE entity must not allow the consumer to make a binder payment until the SVI has been resolved and the PPS has been released to the issuer.
 - ii. The consumer's coverage effective date is in the future.
 - iii. For dental plans only, the consumer's dental policy has a guaranteed premium.

14 Legacy DE Services – Fetch Eligibility and Submit Enrollment

14.1 Fetch Eligibility

The Fetch Eligibility API is a legacy DE service, originally used by Classic DE (aka double-redirect) entities to retrieve eligibility information after a consumer submits an eligibility application. The Fetch Eligibility API is an XML-based API, unlike the newer EDE APIs, which are all JSON-based. EDE entities may find that they can retrieve much of the same information that is returned in the Fetch Eligibility API response via other EDE APIs, in particular via the SES (Get App and Submit App), Get Enrollment, and Get SVI API responses. Although EDE entities can retrieve much of the same data returned in the Fetch Eligibility response via the aforementioned EDE APIs, EDE entities will find that they still need to use the Fetch Eligibility API in some instances. EDE entities should review the below sub-sections for relevant information.

EDE entities can find all of the relevant information pertaining to the Fetch Eligibility service in the DE API Specs and Hub Business Service Definition (BSD) available on zONE at <https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials>. EDE entities should familiarize themselves with the information in the DE API Specs, as there is important guidance in that document, including guidance on age rating, tobacco rating, Plan Category Limitations, APTC distribution, etc.

14.1.1 Variable Eligibility Data

While EDE entities can retrieve much of the data that is returned in the Fetch Eligibility response via other EDE APIs, EDE entities should note that the Fetch Eligibility API is the only API that will refresh variable eligibility data upon subsequent calls when a CIC has not occurred since the last request for variable eligibility data. Variable eligibility data includes things like effective date, max APTC, Plan Category Limitations, etc. Variable eligibility data may need to be refreshed in certain scenarios, and EDE entities may therefore want to use the Fetch Eligibility API in at least some scenarios to retrieve variable eligibility data. For example, if a consumer were to submit an eligibility application on an EDE entity's site, and then leave before completing enrollment, the EDE entity would want to ensure they are using current variable eligibility data if the consumer returns on a subsequent day to complete enrollment. Previously retrieved variable eligibility may no longer be valid in this scenario, for a number of reasons. For example, if a consumer has had a birthday between application submission and enrollment

selection, their max APTC may need to be recalculated based on their new age. Or for example, as time passes between application submission and enrollment selection, the effective date of the enrollment may change based on effective date logic.

EDE entities that choose to use an EDE API such as Get App to retrieve variable eligibility data, instead of Fetch Eligibility, must account for the fact that the EDE APIs don't refresh variable eligibility data. Because of this, EDE entities using an API such as Get App to retrieve variable eligibility data should only consider the API response valid the same day an application is submitted. If a consumer returns on a subsequent day, after submitting an application, an EDE entity would need to have the following logic in place to verify that the variable eligibility data retrieved from an EDE API besides Fetch Eligibility on a prior day is still valid:

- 1) Has the number of available silver plans in the consumer's rating area changed since the application submission date/time in which the EDE API response was retrieved?
- 2) Has any applicant's age as of the effective date changed since the application submission date/time in which the EDE API response was retrieved?
- 3) Is the previously retrieved effective date accurate based on OE and/or SEP effective date rules?
 - If the answer to #1 or #2 is, "yes," the EDE entity should resubmit the application and make a fresh EDE API call in order to retrieve the updated eligibility information, prior to submitting the consumer's Submit Enrollment request.
 - If the answer to #3 is, "no," the EDE entity should have logic in place to calculate the correct effective date for the Submit Enrollment request.
 - If the answer to #1 and #2 is, "no," and the answer to #3 is, "yes," an EDE entity can consider the EDE API response still valid.

14.1.1.1 Non-SEP CIC Effective Dates – SES API Responses

EDE entities should be aware that the finalQhpEffectiveStartDate returned by the SES Submit App and Get App responses may not be accurate in non-SEP CIC scenarios. EDE entities may therefore want to use the EarliestQHPEffectiveDate returned by the Fetch Eligibility API response in, at minimum, non-SEP CIC scenarios.

14.1.2 Plan Category Limitations (aka Metal Level Plan Restrictions)

Plan Category Limitations (aka Metal Level Plan Restrictions) limit the ability for existing consumers to switch plans when reporting SEPs outside of Open Enrollment. Depending on an existing consumer's circumstances, they may be restricted to their current plan, to their current metal level tier, or to specific metal level tiers when reporting SEPs outside of Open Enrollment. In order to properly inform EDE entities of a consumer's Plan Category Limitations, the Fetch Eligibility response will include data elements related to any Plan Category Limitations that apply. Using these data elements, EDE entities will need to implement logic as part of their plan compare experience, to appropriately restrict a consumer's ability to switch plans when reporting SEPs outside of Open Enrollment. EDE entity requirements related to Plan Category Limitations are outlined in Appendix D of the DE API Specs available on zONE at <https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials>.

Note that the DE API Specs outline the data elements that would be applicable in the Fetch Eligibility response, however the Get App, Submit App, and Get Enrollment responses also include data elements relevant to Plan Category Limitations:

- **currentPlanOnlyIndicator** – Can be found in the Submit App and Get App responses.
- **allowedPlanMetalLevelType** – Can be found in the Submit App and Get App responses.
- **planMetalLevelRestrictionRuleType** – Can be found in the Submit App and Get App responses. When the planMetalLevelRestrictionRuleType includes one of the following enumeration values, this will be equivalent to the DependentSEPOrNewMemberIndicator being true in the Fetch Eligibility response:
 - NEW_ENROLLEE_SEP_APP
 - DEPENDENT_MEMBER_TRIGGERING_DEPENDENT_SEP
- **metalTierType** – Can be found in the Get Enrollment response. Equivalent to the Fetch Eligibility CurrentMetalLevelType.

14.1.3 Get App Address Requirement – Phase 3 EDE Entities Only

Phase 3 EDE entities should be aware that the Fetch Eligibility response only returns address data for the primary contact on the eligibility application. Phase 3 EDE eligibility applications however allow consumers to enter different home addresses. As a result, Phase 3 EDE entities are required to obtain address data for each applicant from the Submit App or Get App response (result.computed.members.[Member ID].residencyAddress) instead of from the Fetch Eligibility response. This requirement will allow Phase 3 EDE entities to accurately display plan availability for individual applicants in their shopping experience and apply the corresponding QHP business rules. For example, if a household consisted of parents and a child in college, and the parents and child indicated different home addresses on the eligibility application, the parents and child may not have the same plan availability. If a Phase 3 EDE entity were using Fetch Eligibility to obtain address data in this scenario, the EDE entity may encounter an unnecessary Submit Enrollment failure if the parents and child attempted to enroll in a plan that wasn't allowed based on each of their respective residency addresses.

14.1.4 Allocation of APTC to Enrollment Groups

When allocating APTC to enrollment groups for the Submit Enrollment request, there are a number of considerations that need to be made by an EDE entity. These considerations are outlined in Appendix C of the DE API Specs available on zONE at <https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials>.

EDE entities should note that the Submit App and Get App responses only return a single maxAPTCAmount for the entire household, and do not provide prorated individual APTC amounts based on the uniform age rating curve for each applicant in the household the same way that Fetch Eligibility does. The prorated APTC amounts are particularly important in scenarios where there are multiple enrollment groups, and EDE entities will therefore likely want to retrieve this information from the Fetch Eligibility response. Note that EDE entities are required to support households this wish to enroll in separate plans and/or enrollment groups.

14.2 Submit Enrollment

The Submit Enrollment API is a legacy DE service, originally used by Classic DE (aka double-redirect) entities to submit an enrollment after a consumer submits an eligibility application. The Submit Enrollment API is an XML-based API, unlike the newer EDE APIs, which are all JSON-based. At this time, the Submit Enrollment API is still the standard enrollment service for both Classic DE and EDE. EDE entities will need to integrate with this service as part of their EDE implementation, if they are not already integrated with the service. EDE entities can find all of the relevant information pertaining to the Submit Enrollment API in the DE API Specs and Hub Business Service Definition (BSD) available on zONE at <https://zone.cms.gov/document/direct-enrollment-de-documents-and-materials>. EDE entities should be sure to familiarize themselves with the information in the DE API Specs, as there is important guidance in that document, including guidance on age rating, tobacco rating, Plan Category Limitations, APTC distribution, etc.

15 Event-Based Processing (EBP)

15.1 Event-Based Processing Overview

The Event-Based Processing API allows EDE entities to ingest certain business events that occur for their consumers in near real time, making it possible for EDE entities to take over messaging for the applicable events. For example, using the EBP API, EDE entities can identify when an SVI or DMI has been created or resolved for a consumer, when the consumer has provided insufficient documentation to resolve an SVI or DMI, when a 1095-A is available for the consumer, etc. For a full list of events that are available via the EBP API, EDE entities should view the EBP API Specs available on zONE at <https://zone.cms.gov/document/enhanced-direct-enrollment-edo-documents-and-materials>. Note that the EBP API is an optional API, and EDE entities are not required to integrate with this API.

Below is some pertinent information that EDE entities should be aware of when using the EBP API:

- EDE entities will submit API requests to ingest events on regular and frequent interval.
 - There is a maximum API request rate of one API request every 20 seconds.
- The maximum number of events that will be returned in a single API call is 2,000.
- EDE entities are required to use the CONSUMER_DE Role-Id when using the EBP API, and are also required to use a User-Id that represents the EDE entity's system (i.e. this shouldn't be a consumer or agent/broker User-Id, but instead something to represent the EDE entity's system, like EDEPartnerXSystem, for example).
- EDE entities will only have access to events generated for applications and policies that they have permission for at the time the API request is sent.
- EDE entities are permitted to leverage the Get App API to retrieve any additional metadata that is necessary for email communication (i.e. consumer's name, email address, preferred written language, etc.).

-
- EDE entities may want to maintain record of certain data that can be used in coordination with the EBP API events.
 - For example, tracking of SVI and DMI end dates, which can be used for “chase campaigns” until an event is received to indicate the SVI or DMI is resolved.
 - Some events do not have a corresponding email action, and therefore EDE entities may not need to take any action in response to the event.
 - For example, when an application is created, the FFM does not currently generate an email that goes out to the consumer.
 - This type of event may therefore be more of an informational event for the EDE entity.
 - Some events may be the result of something that has occurred that the EDE entity is already aware of.
 - For example, when an enrollment/policy is created, the EDE entity will know this through both the Submit Enrollment response and the EBP API response.
 - EDE entities may choose to ignore the EBP event if appropriate messaging already exists when a Submit Enrollment response is successful.

15.2 Email Toggle Functionality

In addition to the EBP API, CMS has also implemented “Email Toggle Functionality”. This functionality enables CMS to turn off emails generated by HealthCare.gov once an EDE entity has been approved to take over one or more event-related email.

15.2.1 EDE Requests to Disable FFM-Generated Emails

EDE entities that wish to integrate with the Event-Based Processing API and take over specific email communications from HealthCare.gov, must submit the following documentation:

- An “EDE Request to Disable FFM-Generated Emails”.
 - This form can be found on zONE at <https://zone.cms.gov/document/business-audit>
- In addition to the “EDE Request to Disable FFM-Generated Emails”, EDE entities that would like to request that CMS disable specific emails generated by HealthCare.gov, will also need to submit the following supporting documentation:
 - An overview of the EDE entity’s communications strategy, including:
 - A technical description of the systematic process the EDE entity will use to generate and send emails in response to events being ingested via the Event-Based Processing API.
 - The interval in which the EDE entity will ingest events from the Event-Based Processing API.
 - For example, will events be ingested from the Event-Based Processing API every 20 seconds, every 6 hours, etc.?

-
- The interval in which the EDE entity will send consumer emails after ingesting corresponding events from the Event-Based Processing API.
 - For example, will consumer emails be generated simultaneously when an event is ingested from the Event-Based Processing API, will consumer emails be aggregated and sent at certain points in the day, etc.?
 - A description of how the EDE entity will store email-related data, such as the date and time an email was sent, for audit purposes
 - Examples of each email type that will be generated by the EDE entity, for the specific email groups (see [below](#)) that the EDE entity is requesting be disabled on the FFM.
 - If the EDE entity will combine email communications, when applicable, the EDE entity should also provide examples of the combined emails.
 - For example, if an event is received for both application submission and DMI creation, and the EDE entity will combine the consumer communication into one email, the EDE entity should provide an example of the combined email.
 - If the EDE entity's platform is available to consumers in a state where a non-English language is spoken by a limited English proficient (LEP) population that reaches 10 percent or more of the population for the relevant state, as determined in guidance published by the Secretary of HHS, then the EDE entity must also submit an example of each email type that will be generated when there is a relevant non-English language communications preference for a consumer in these states.
 - For example, if the EDE entity plans to offer an EDE pathway for consumers in Texas, the EDE entity must provide Spanish-language examples of the emails that will be generated for consumers that have a Spanish-language communications preference.

Note that both the “EDE Request to Disable FFM-Generated Emails” and the supporting documentation will need to be submitted to CMS via the Secure Portal. When submitting these documents via the Secure Portal, EDE entities should enter “EDEORRTeam@bah.com” in the “To” line, and also include “[EDE Entity Name]: EDE Request to Disable FFM-Generated Emails” as the subject line. EDE entities should replace “EDE Entity Name” with the name of the EDE entity that is submitting the request.

15.2.2 EDE Entity Email Requirements and Recommended Best Practices

EDE entities that take over email communications for their consumers should be aware of the following emails requirements:

-
- Language used in emails needs to be consistent and similar to content required in HealthCare.gov email, and must be in alignment with any EDE requirements outlined in the EDE auditor Toolkits.
 - No acronyms should be used.
 - No internal terms should be used (i.e. SEP Verification Issue).
 - Emails should include actionable deadlines and content.
 - Note, example HC.gov emails can be found on zONE at <https://zone.cms.gov/document/business-audit>
 - When there's a notice available that needs to be viewed, this should be communicated in the email to the consumer. Note, most HealthCare.gov transactional emails are triggered by a status change and have an associated notice that the consumer needs to read. There is a legal requirement to deliver an electronic communication tied to a notice when the consumer has selected electronic preferences in their application.
 - Emails & SMS text messages need to be transactional, especially when a notice has been generated. These communications need to be triggered in as close to real-time as possible, but no more than 24 hours after a notice has been generated. Notices often contain deadlines, which the consumer needs to be informed about quickly so they have an opportunity to respond.
 - EDE entities need to store and maintain records related to emails and text messages sent and delivered tied to notices, and must be able to provide the records to CMS upon request to assist with appeals, casework, and other inquiries.
 - EDE entities must be sure to protect PII and sensitive eligibility/enrollment information. Emails can contain a limited amount of PII to help personalize and communicate about actions and deadlines, however, emails must not include the notice itself as an attachment.
 - EDE entities must make it clear how consumers can opt-out of or stop communications; this includes guiding consumers to update their notice delivery preferences in their application. If consumers opt out of receiving emails or text messages, their application needs to be updated to change their response for notice delivery so that the consumer will then receive mailed paper notices. EDE entities can maintain different preferences for Marketplace communications and other non-Marketplace entity outreach activities. If permission is revoked at any time, EDE entities must stop sending communications related to the consumer's application or enrollment status, action items and activities.

In addition to the above requirements, EDE entities taking over emails communications for their consumers should be aware of the following recommended best practices:

- Email Subject lines should be action-driven.
- Content should be specific to the item(s) being communicated. For example, DMI and SVI Creation, or DMI and SVI Reminders can be combined into one email about both,

but the email needs to still communicate that the consumer needs to send additional information for the specific DMIs and SVIs along with each deadline.

- EDE entities should include deep-links when possible, where when the consumer selects the link, they are forced to log in and then subsequently they land on the specific page with more information/status with access to download their notice(s).
- SMS text messages should be actionable to drive the consumer to log in, take action, and review their notices for more information.
- EDE entities should include personalization and coverage year context. Consumers may be getting emails about 2019 and 2020 actions in the same time period, for example, so the EDE entity should make sure to include which year the email relates to.
- EDE entities should update dynamic content and context throughout the year.

Example Subjects

- Action needed to finalize your enrollment
- Take action to keep your coverage
- Upload your documents today
- Confirm your move: we need more information
- Take the last step: send documents
- Get ready for Open Enrollment

Example information

- You need to confirm your income – send documents by June 23, 2019
- You need to confirm Sam’s move – send documents by May 16, 2019
- You need to confirm the following information:
 - By May 23, 2019 send documents for
 - Sam’s move
 - Heather’s loss of other coverage
 - By June 23, 2019 send documents for
 - Sam and Heather’s income
 - Heather’s citizenship
 - The Marketplace reviewed your documents, but still needs more information to confirm your household’s income by June 23, 2019. Log in now to read your notice.

15.2.3 Email Groups

CMS would like to ensure that as we transition communications off the HealthCare.gov platform, that entire email groups are moved at one time. For example, we expect that all SVI and DMI related communications will be transitioned over to an EDE entity at one time, so that

consumers aren't some of those communications from the EDE entity, while still getting some of the communications from HealthCare.gov for the same topic.

When an EDE entity is ready to take over a group of communications, CMS will toggle off the transactional (system-triggered) communications from HealthCare.gov, and will also suppress any customer service (i.e. "chase campaigning") emails/texts tied to that email group, such as deadline reminder emails for various actions.

Below are the current email groups that an EDE entity request be disabled by CMS:

- **Application Email Group:**
 - Application Submission Email
- **Verification Issues Email Group:**
 - SVI Created Email
 - SVI Resolved Email
 - SVI Expired Email
 - SVI Obsolete Email
 - SVI Insufficient Documentation Email
 - DMI Created Email
 - DMI Resolved Email
 - DMI Expired Email
 - DMI Escalation Email
 - DMI Insufficient Documentation Email
 - SVI and DMI Deadline Reminders
- **Consumer Information Email Group:**
 - Initial 1095-A Email
 - Corrected 1095-A Email
 - Voided 1095-A Email
- **Enrollment Email Group:**
 - Plan Selection Email

16 Update Policy

16.1 Update Policy Overview

The Update Policy API allows EDE entities to initiate specific actions that impact a consumer's existing policy or Pended Plan Selection (PPS). The initial production rollout of the Update Policy API on 3/20/2020 will include functionality that allows EDE entities to cancel or terminate a consumer's existing policy or PPS upon the consumer's request to do so. On 5/1/2020, BAR opt-out functionality will also be deployed to production, which EDE entities can leverage through the Update Policy API when a consumer indicates they don't want their coverage automatically renewed for the upcoming plan year. CMS intends to add additional functionality to the Update Policy API in the future, and updates to the EDE API Companion Guide will be made as necessary. Required EDE entity implementation dates for Update Policy

functionality will be outlined in the EDE CMS-Initiated CR Tracker available on zONE at <https://zone.cms.gov//document/enhanced-direct-enrollment-edo-documents-and-materials>.

16.2 Update Policy API – Cancellation/Termination Business Rules

When integrating with the cancellation/termination functionality available via the Update Policy API, EDE entities should familiarize themselves with the business rules outlined below. Similar to the cancellation/termination functionality currently available in the HealthCare.gov My Account space, the cancellation/termination functionality available via the initial rollout of the Update Policy API has certain limitations. Business rules that EDE entities should be familiar with related to the Update Policy API and associated cancellation/termination functionality are outlined below:

- EDE entities will need to use the Get Enrollment API to determine which coverage exists and subsequently which can be cancelled/terminated.
- If cancelling or terminating health coverage, the Update Policy API request will only allow for cancellation or termination of all active health policies at one time.
 - In other words, if multiple active health policies exist, a user will not be able to cancel or terminate an individual health policy; all health policies will need to be cancelled or terminated at the same time.
- If cancelling or terminating health or dental coverage, only the entire health or dental policy can be cancelled.
 - In other words, the initial implementation of the Update Policy API will not allow for member-level cancellation or termination of coverage.
- The Update Policy API will allow for cancellation or termination of an individual dental policy, when multiple active health and dental policies exist.
 - The Update Policy API will not however allow for dental-only coverage.
 - In other words, if multiple health and dental policies exist, the health coverage cannot be cancelled or terminated without also cancelling or terminating the dental coverage.
- The FFE will derive whether the action is a cancellation or a termination based on the actionEffectiveDate provided in the Update Policy API request, however EDE Partners should be aware of the following:
 - Cancellation of a policy can only occur up until the coverage start date of the policy; the actionEffectiveDate for a cancellation will need to be either the coverage start date, or the day prior to the coverage start date.
 - Termination of a policy can occur after the coverage start date, but the termination cannot be applied retroactively; the actionEffectiveDate for a termination will need to be either the date the termination is initiated or a future date. EDE entities should allow their users to select a termination date of their choice, as long as the termination date is valid based on this rule.

-
- Cancellation of a Pended Plan Selection (PPS) can occur at any point while the PPS is still active; the actionEffectiveDate for a cancellation will need to be either the coverage start date, or the day prior to the coverage start date.
 - In the event that a consumer has a future termination date for their dental coverage, and the consumer requests to cancel or terminate their health coverage for an earlier date, the EDE entity must ask the consumer within their UI whether they would also like to cancel or terminate their dental coverage for the earlier date.
 - The Update Policy API will allow the dental termination date to be shifted to an earlier date, as long as the requested cancellation or termination date doesn't violate any of the previously mentioned business rules.
 - Example: On 12/15, a consumer enrolls in both a health and dental policy, effective 1/1.
 - On 3/1, the consumer uses an EDE site to terminate their dental policy only, effective 4/30.
 - On 3/15, the consumer uses an EDE site to terminate their health policy, effective 3/31.
 - At this time, the consumer must be given the option to also terminate their dental policy, effective 3/31.
 - Issuer EDE entities should take note of the exception outlined below.
 - In situations where a consumer or a consumer's agent/broker is working with an EDE issuer, and the consumer has a PPS or policy that is not owned by the EDE issuer, the EDE issuer is permitted to either:
 - Display available details for the PPS or policy in the issuer's UI, and allow the user cancel or terminate the PPS or policy.
 - Note, EDE issuers may only receive limited details for the PPS or policy in the Get Enrollment response.
 - Or alternatively, display messaging to the user indicating that a PPS or policy exists that is owned by a different issuer, and that the user can go to HealthCare.gov or the FFE Call Center to cancel or terminate coverage.

EDE entities can find the Update Policy API Specs on zONE at <https://zone.cms.gov//document/enhanced-direct-enrollment-edo-documents-and-materials>.

16.3 Update Policy API – BAR Opt-Out Business Rules

When integrating with the BAR opt-out functionality available via the Update Policy API, EDE entities should familiarize themselves with the business rules outlined below:

- EDE entities will need to use the Get Enrollment API to determine which active policies exist and subsequently which policies are eligible for BAR opt-out.
 - EDE entities should note that Pended Plan Selections are not eligible for BAR opt-out.

- EDE entities should also note that policies with a specifiedEoyEndDateIndicator of true, or a cancellation/termination date earlier than 12/31, will not be eligible for BAR opt-out.
- EDE entities will need to use the System Reference Data API to determine when BAR opt-out should be displayed for eligible consumers, based on the configurable BAR opt-out period returned in the System Reference Data API response.
- If a consumer is opting out of BAR, note that the initial Update Policy BAR opt-out functionality will only allow the consumer to opt out of BAR for all existing policies tied to the application. This mirrors the existing HealthCare.gov My Account BAR opt-out functionality.
 - In other words, policy-level and member-level BAR opt-outs are not currently supported.
- In situations where a consumer or a consumer’s agent/broker is working with an EDE issuer, and the consumer has a policy that is eligible for BAR opt-out that is not owned by the EDE issuer, the EDE issuer is permitted to either:
 - Display available details for the policy in the issuer’s UI, and allow the user to opt out of BAR for the policy.
 - Note, EDE issuers may only receive limited details for the policy in the Get Enrollment response.
 - Or alternatively, display messaging to the user indicating that a BAR-eligible policy exists that is owned by a different issuer, and that the user can go to HealthCare.gov or the FFE Call Center to opt out of BAR.

The below table outlines when BAR opt-out would be displayed in the UI, along with the outcome of the BAR opt-out:

Scenario Description	Display BAR Opt-Out?	Result of BAR Opt-Out
Application with: <ul style="list-style-type: none"> ● No policies tied to it 	No	<ul style="list-style-type: none"> ● N/A
Application with: <ul style="list-style-type: none"> ● No active policies tied to it (i.e. cancelled or terminated policies only) 	No	<ul style="list-style-type: none"> ● N/A
Application with: <ul style="list-style-type: none"> ● Active policies tied to it, but outside of configurable BAR opt-out window 	No	<ul style="list-style-type: none"> ● N/A
Application with:	Yes	<ul style="list-style-type: none"> ● Current year policy is terminated with a 12/31

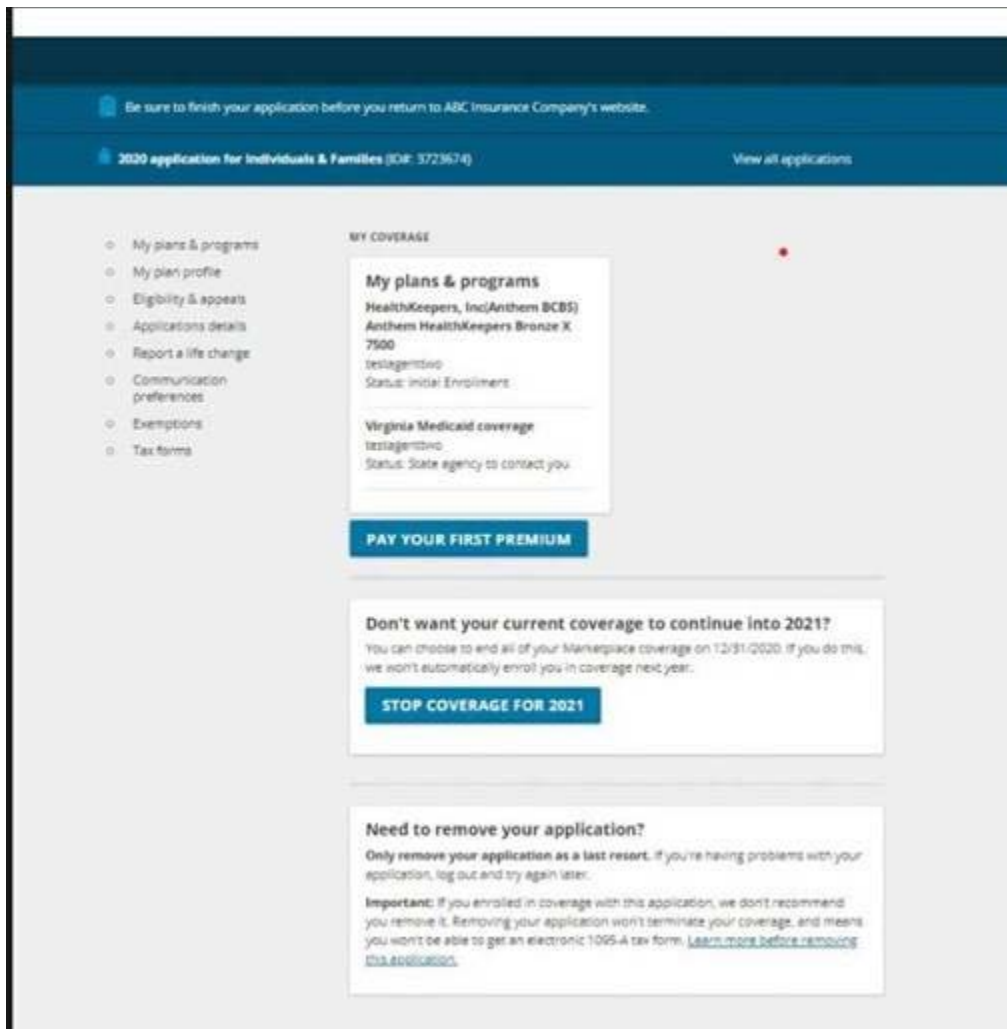
<ul style="list-style-type: none"> • Active policies tied to it, and inside of configurable BAR opt-out window <ul style="list-style-type: none"> ○ BAR has not occurred ○ Policy has a specifiedEoyEndDateIndicator of false ○ Policy has a insurancePolicyEndDate equal to 12/31 		<p>termination date (EOY indicator = true)</p> <ul style="list-style-type: none"> • BAR will not be processed
<p>Application with:</p> <ul style="list-style-type: none"> • Active policies tied to it, and inside of configurable BAR opt-out window <ul style="list-style-type: none"> ○ BAR has occurred ○ Policy has a specifiedEoyEndDateIndicator of false ○ Policy has a insurancePolicyEndDate equal to 12/31 	<p>Yes</p>	<ul style="list-style-type: none"> • Current year policy is terminated with a 12/31 termination date (EOY indicator = true) • Future year BAR policy is cancelled

EDE entities can find the Update Policy API Specs on zONE at <https://zone.cms.gov//document/enhanced-direct-enrollment-edo-documents-and-materials>.

16.3.1 BAR Opt-Out Messaging

EDE entities integrating with BAR opt-out functionality must display appropriate messaging to users within their UI, so that users understand that their coverage won't be automatically renewed when they elect to opt out of BAR. Below are example screenshots from the HealthCare.gov UI that include language that EDE entities may want to use as a model for their own BAR opt-out language.

HealthCare.gov My Account screenshot showing the "Stop Coverage for 2021" (i.e. BAR opt-out) button:



Example of messaging displayed in the HealthCare.gov My Account when the BAR opt-out button is selected:

You've chosen to stop your Marketplace coverage for 2020

Your Marketplace coverage in these plans will end on 12/31/2019:

- Silver Perks

We won't automatically enroll you in coverage next year. **If you want Marketplace coverage in 2020**, you'll need to complete an application during Open Enrollment.

I understand that I'm ending Marketplace coverage for all members of my household after December 31, 2019, and the Marketplace won't automatically enroll me in coverage for 2020.

[GO BACK](#) [STOP COVERAGE FOR 2020](#)

After a user elects to opt out of BAR, EDE entities may also want to display language in the UI reminding the user that they have opted out of BAR. For example, the EDE entity may want to leverage the `insurancePolicyEndDate` and `specifiedEoyEndDateIndicator` in the Get Enrollment response to identify when a user's coverage will not be auto-renewed. When the `insurancePolicyEndDate` equals 12/31 of the given coverage year and the `specifiedEoyEndDateIndicator` is true, the EDE entity might want to display something like, "You won't automatically be enrolled in coverage next year. Your Marketplace coverage will end on December 31, 2020. If you want Marketplace coverage in 2021, you'll need to complete an application during Open Enrollment."

Below is an example of what is displayed on the HealthCare.gov eligibility results page when BAR opt-out has occurred:

Optional: Stop Marketplace coverage for 2020

Your Marketplace coverage will end on December 31, 2019 and we won't automatically enroll you in coverage for 2020.

17 Performance Testing

17.1 Performance Testing Overview

After an EDE entity completes their EDE UI build and integrates with all of the necessary EDE APIs, the EDE entity may wish to conduct performance testing of their EDE platform. CMS will permit EDE entities to conduct performance testing, however, performance testing must only be conducted in CMS' IMP1B testing environment. EDE entities must not conduct performance testing in any other environment, as IMP1B is CMS' performance testing environment, and it is scaled for production-like activity, whereas our other testing environments are not scaled to handle production-like loads.

If an EDE entity would like to conduct performance testing in IMP1B, the EDE entity should send an email to Joshua.Halsey@cms.hhs.gov with the subject line, "Request to Conduct EDE Performance Testing". Requests should be submitted at least one week in advance of the date being requested for performance testing. Requests should also include the dates and times requested for testing. Generally, CMS will schedule a 4 hour window for testing on a given day, but EDE entities can request more than 4 hours if necessary. CMS will try to accommodate the dates and times requested, but will provide alternate options if there is conflicting testing already scheduled. EDE entities should generally expect a response within 48 business hours after submitting a request to test, with either confirmation of the testing window, or with alternate options if the timeslot requested is already reserved.

EDE entities should also be aware of the following after scheduling a performance testing timeslot:

- If an EDE entity needs to cancel the reserved performance testing timeslot, the EDE entity should do so at least 24 hours in advance, if at all possible. The cancellation request should be sent to Joshua.Halsey@cms.hhs.gov.
- The Hub will provide the EDE entity with the Partner ID, password, and endpoints to use for testing prior to the reserved testing timeslot.
 - CMS recommends that EDE entities test connectivity at least one business day before their scheduled testing timeslot.
 - If an EDE entity encounters connectivity issues, the EDE entity should email Hubsupport@sparksoftcorp.com.
- EDE entities must email Joshua.Halsey@cms.hhs.gov at the start and end of their testing.
- EDE entities should also note that CMS always reserves the right to cancel EDE entity testing, due to a critical need on the CMS side.
 - CMS will notify the EDE entity at least 24 hours in advance if cancellation is necessary, when at all possible.

Appendix A: Acronyms and Abbreviations

Acronym / Abbreviation	Literal Translation
API	application Programming Interface
APTC	Advanced Premium Tax Credit
ANSCA	Alaska Native Claims Settlement Act
CIC	Change in Circumstance
DOB	Date of Birth
FED	Federal
FEIN	Federal Employer Identification Number
FFM	Federally Facilitated Marketplace
EDE	Enhanced Direct Enrollment
HIOS	Health Insurance Oversight System
HUB	Data Services Hub
IPP	Insurance Plan Policy
JSON	JavaScript Object Notation
M834	Maintenance 834
NPN	National Producer Number
QHP	Qualified Health Plan
SEDI	Sliding Effective Date Indicator
SEP	Special Enrollment Period
SVI	SEP Verification Issue
SADP	Stand Alone Dental Plan
PPS	Pended Plan Selection
UI	User Interface
URI	Uniform Resource Indicator
XML	Extensible Markup Language

Appendix B: Referenced Documents

Document Name	Document Number and/or URL	Issuance Date

Draft