Emergency Triage, Treat, and Transport (ET3) Model

ET3 Model Data Submission Guide for NEMSIS 3.4 Support, 2nd Ed.

January 2022

Table of Contents

Acknowledgement

The Emergency Triage, Treat, and Transport (ET3) Model acknowledges the support and collaboration of the National Highway Traffic Safety Administration (NHTSA) Office of Emergency Medical Services (OEMS) and the National Emergency Medical Services Information System (NEMSIS) Technical Assistance Center (TAC). Both this revised guide, and the ET3 Model data submission process that it covers, would not be what they are without this partnership.

Overview

The ET3 Model requires that Participants regularly submit data in addition to the Medicare claims information used as part of billing for ET3 Model Interventions. NEMSIS standard electronic Patient Care Report (ePCR) data are an important and large component of ET3 Model data submissions. NEMSIS standard ePCR data are a new quantitative data source for the ET3 Model and the Center for Medicare and Medicaid Innovation (CMMI) at the Centers for Medicare and Medicaid Services (CMS). However, the data source is very familiar to participating EMS ambulance suppliers and providers, and their supporting software vendors. Thus, the main goal of this guide is to familiarize Participants and their supporting vendors with the submission of NEMSIS version 3.4 ePCR data into ET3 Model systems and confirmation that the ET3 Model has correctly received that data. This guide assumes familiarity with the NEMSIS standard specifications and readers are encouraged to contact the NEMSIS TAC with any questions about those specifications.

NEMSIS standard ePCR data will benefit both the ET3 Model and Participants. For the ET3 Model, ePCR data will be used in Model monitoring and evaluation. A consistent data format will enable CMS to aggregate data across the Model and provide Participants with feedback and assistance implementing Model interventions.

Submission of ePCR data is divided into two periods: initial submission and subsequent submissions. (Note: additional information on data submission requirements can be found in Article 16 of the ET3 Model Participation Agreement.)

The initial ePCR submissions were initially due on April 30, 2021. These submissions were composed of two sets of ePCR data. The first component was all participating EMS agencies' ePCRs generated from March 2019 to February 2020. These data will be used to form a standard baseline for all agencies before both the coronavirus disease 2019 (COVID-19) national public health emergency and the ET3 Model altered their operations. The second component was all participating EMS agencies' ePCRs generated in January to March 2021. These data covered the first three months of ET3 Model performance.

Subsequent ePCR submissions are due on the last day of each calendar month, starting on March 31, 2021. These submissions will be composed of all participating EMS agencies' ePCRs generated in the *previous* calendar month. For example, all of the ePCRs generated in September 2021 are due by October 31, 2021. All of the ePCRs generated in October 2021 are due by November 30, 2021 and so forth for each month during participation in the ET3 Model. ePCRs may be submitted before the due date and they are expected to be submitted in real time using the NEMSIS web services description language (WSDL)/application programming interface (API) transmission standard.

Roles and Responsibilities

Several entities play roles in providing the necessary tools, processes, and techniques for fulfilling the ET3 Model data submission requirements.

ET3 Model Participants

ET3 Participants are entities that have signed and executed ET3 Participation Agreements to provide ET3 Model Interventions to Medicare Fee-for-Service beneficiaries. The Participant is responsible for collecting ePCR data in the NEMSIS standard and submitting that ePCR data to the ET3 Model. Submission of ePCRs to the ET3 Model is in addition to—not in lieu of—Participants' existing data submission requirements to other regulatory entities, such as local and state governments.

Participants may send the ePCR data directly to CMS or with the support of NEMSIS-compliant ePCR software vendors.

NEMSIS-compliant ePCR Software Vendors

NEMSIS-compliant ePCR software vendors are permitted to submit ePCR data to CMS on behalf of Participants. Any software vendors supporting Participants are encouraged to closely coordinate their ePCR submission processes with the ET3 Model and the NEMSIS TAC.

Software vendors can play vital roles in ePCR submissions to the ET3 Model, but their supported Participants maintain final responsibility for meeting the ET3 Model data submission requirements.

NEMSIS Technical Assistance Center

NEMSIS provides the framework for collecting, storing, and sharing standardized EMS data. NEMSIS is both a universal standard for how patient care information resulting from an emergency 911 call for assistance is collected and the national database used to store EMS data from signatory US states and territories.

The ET3 Model has partnered with the NEMSIS TAC to assist the Model's adoption of NEMSIS data standards and provide related technical support. For example, the NEMSIS TAC assisted the ET3 Model with the development of the ET3 Schematron schema for validating ePCRs and with delivering technical information to ePCR software vendors.

CMMI at CMS

CMMI develops new payment and service delivery models in accordance with the requirements of Section 1115A of the Social Security Act. The ET3 Model is one of several models that require the exchange of patient data between the medical community and CMS. CMMI has provided the platform and technologies required to accept ePCR data from Participants.

CMMI will then analyze the ePCR data collected as part of the ET3 Model to support its ongoing statutory mission, including Participant performance, payment monitoring, and Model evaluation.

ET3 Model Help Resources

In addition to their assigned ET3 Model Project Officers, Participants have access to Help Desks for questions throughout their participation in the ET3 Model.

- The ET3 Mailbox is available for general ET3 Model questions via ET3Model@cms.hhs.gov.
- The ET3 Help Desk is available for all data submission *technical* questions via 1-844-711-2664.

Required Data Submissions

NEMSIS Standard ePCR Data for the ET3 Model

The ET3 Model will require Participants to submit ePCRs that are compliant with current NEMSIS versions. As of June 2021, NEMSIS versions 3.4.0 and 3.5.0 are current. The NHTSA OEMS and the NEMSIS TAC are scheduled to stop supporting (“sunset”) NEMSIS version 3.4.0 in January 2024. ET3 will adopt a similar data submission compliance schedule: ET3 will accept ePCR submissions in both versions 3.4.0 and 3.5.0 during the implementation period, then ET3 will accept only ePCRs in version 3.5.0 once the NEMSIS TAC has sunset version 3.4.0.

Much of what Participants and their supporting software vendors already know and do for ePCR submissions remains the same for ET3 Model data submissions. The ET3 Model took this approach of making limited customizations to facilitate and streamline the data submission process and to provide common data standards for a national model while accommodating agencies’ respective state data regulations.

The ET3 Model will apply the same standard structure of NEMSIS ePCR elements and the data validations for the XSD and National Schematron schemas. The ET3 Model will collect all Mandatory data elements, but there are some Required and Recommended data elements that the ET3 Model will not collect. There also are some Optional elements that the ET3 Model will collect. It is important to note that the ET3 Model has not made any changes that conflict with the XSD and National Schematron schemas. The XSD and National Schematron validation schemas will be applied to ePCR data submissions that the ET3 Model receives with no changes, additions, or deletions to the existing “Errors,” “Warnings,” and status codes.

The ET3 Model will require Participants to apply some limited customizations to version 3.4.0 ePCR submissions in order to help appropriately document the ET3 Model’s Interventions.

First, the ET3 Model has a list of NEMSIS data elements that are to be collected. The list includes all of the elements that are “Mandatory” in the NEMSIS data standard, plus additional standard NEMSIS elements. The list of data elements collected by the ET3 Model can be found in Appendix B. Participants may submit NEMSIS elements that are not on the ET3 Model list, but the ET3 Model will not process or store those elements.

Second, the ET3 Model has one custom element (et3Disposition.01) and custom values added to two existing NEMSIS data elements (eDisposition.21 and eDisposition.29). More details on this element and values, including their codes and definitions, can be found in Appendix B.

Third, the ET3 Model has one set of new Schematron rules that will be used to validate ePCRs submitted by Participants. This Schematron schema consists entirely of “Warnings” and will be utilized in a similar fashion as a set of “State” rules applicable to Participants. More details on this ET3 Model-specific Schematron schema can be found in Appendix C.

Finally, the NEMSIS TAC also has resources available for Participants on its website. Participants are encouraged to contact the NEMSIS TAC for technical questions on the NEMSIS standard (https://nemsis.org/using-ems-data/cms-et3-project/).

Medicare Claims Data for the ET3 Model

The ET3 Model will use Medicare claims data generated by Participants and their Partners as a data source. While Medicare claims and ePCRs can be related data and cover the same ET3 Model Intervention/response, this guide will not focus on Medicare claims because those data are submitted through different processes and systems. For further information on Medicare claims data as part of the ET3 Model, Participants are encouraged to refer to the “Participant Billing and Payment Factsheet” available for download on the ET3 Connect Site and reach out their assigned Project Officers with any questions.

Submission Process and Work Flow

Once an ePCR is generated by a Participant, it must be submitted to CMS by the last day of the calendar month following the date of the incident. The Participant is responsible for the data submission into ET3 Model systems, whether directly or through a supporting ePCR software vendor.

As part of the ET3 Model Onboarding process, a participating agency or supporting software vendor will create an account with ET3 Model systems and request the application programming interface (API) keys needed for secure ePCR transmission. After those API keys are issued and test transmissions are confirmed, ePCRs can be submitted.

Participating agencies or their supporting software vendors will submit ePCRs into the ET3 Model’s Centralized Data Exchange (CDX) system. Each ePCR will be validated using the NEMSIS standard XSD and National Schematron schema, as well as the ET3 Model-specific “State” Schematron schema. A status code will be generated for each submission.

Once an ePCR submission passes validation, it will be filtered and only the elements that the ET3 Model requires will proceed to further data processing.

Confirming Data Receipt

ET3 Participants can check the status of their ePCR submissions to the ET3 Model through the CDX Dashboard component of the ET3 application. The steps for accessing this function in CDX are detailed in Appendix E.

Additionally, Participants can reach out to their Project Officers to inquire about submission status.

Frequently Asked Questions

1. What required data elements will Participants need to report? How often? To whom?

   CMS currently requires Medicare claims data and NEMSIS standard ePCR data from Participants. Participants will be notified at least 60 days in advance if CMS changes the required data elements. Please see Overview and Required Data Submissions section(s) in this document for more details on data submission frequency, deadlines, and routes.

2. Why is CMS collecting National Emergency Medical Services Information System (NEMSIS) standard electronic Patient Care Report (ePCR) data for the ET3 Model?

   NEMSIS standard ePCR data is very familiar to participating Emergency Medical Services (EMS) ambulance suppliers, providers, and their supporting software vendors, and will be used in Model monitoring and evaluation. It provides a consistent data format that will enable CMS to aggregate data across the Model, and provide Participants with feedback and assistance implementing Model interventions.

3. Do we need to submit all electronic Patient Care Reports (ePCRs) regardless of payer?

   Yes, ET3 requires the submission of all PCRs generated by Participants for the time periods listed in the Data Submission Guide. Specifically, any ePCR with an eTimes.03 (NEMSIS v3.4) value that falls in the time periods listed is required for submission. Time period submissions and/or deadlines enable the comparison of ET3 interventions to a control group of ePCR records.

4. When will ePCR data be submitted?

   Submission of ePCR data is divided into two periods: Initial Submission and Subsequent Submissions.
   Initial ePCR Submission: *Due April 30, 2021, and will be composed of two sets of ePCR data:*

   1) All participating EMS agencies' ePCRs generated from March 2019 to February 2020; and

   2) All participating EMS agencies' ePCRs generated from January to March 2021.

   Subsequent ePCR Submissions: *Due on the last day of each calendar month, starting March 31, 2021. These submissions will be composed of all participating EMS agencies' ePCRs generated in the previous calendar month.*

   Additional information on data submission requirements can be found in Article 16 of the Participation Agreement.

5. Our organization is not planning to implement ET3 Model Interventions until late 2021. Do we still need to submit initial and subsequent ePCR data?

   ET3 Model Implementation is not required until January 1, 2022. However, the initial ePCR data submission, due April 30th, 2021, was required to establish a baseline for Model participation, regardless of whether you are implementing ET3 Model Interventions. Subsequent data submissions are required on a monthly basis regardless of Model implementation date. If you will have any issues meeting these deadlines, or require technical support, please contact your Project Officer. Please refer to Article 6 of the Participation Agreement regarding Model implementation date, and Article 16 regarding data submission requirements.

6. What are the data submission requirements of the ET3 Participant and their NEMSIS-compliant ePCR software vendor(s)?

   The Participant is responsible for collecting ePCR data in the NEMSIS standard and submitting that ePCR data to CMS, either directly to CMS or with the support of NEMSIS-compliant ePCR software vendor(s). Any software vendors supporting Participants are encouraged to closely coordinate their ePCR submission processes with the ET3 Model and the NEMSIS Technical Assistance Center (TAC Participants maintain final responsibility for meeting the ET3 Model's data submission requirements.

7. Whom should an ET3 Participant contact for assistance around data submission?

   *Participants can contact their ET3 Model Project Officer for all ET3 Model non-technical questions. Email the ET3 Mailbox at **ET3Model@cms.hhs.gov,** and include your Application ID in the format "ET3-0XXX" in the subject line.*

   The Innovation Development and Operations Services (IDOS) Help Desk is available for all ET3 Model data submission technical questions. Call 1-844-711-2664 to reach the IDOS Help Desk.

8. What NEMSIS version standard will Participants need to comply with for ePCR submission?

   The ET3 Model will require Participants to submit ePCRs that are compliant with the NEMSIS version 3.4 or 3.5 standard. The ET3 Model will require Participants to apply some limited customizations to version 3.4 or 3.5 ePCR submissions to help appropriately document the ET3 Model's Interventions.

   1) The ET3 Model has one custom element (eDisposition.01), and has added custom values to two elements (eDisposition.21 and eDisposition.29) for NEMSIS version 3.5.
   2) The ET3 Model has one set of new schematron rules that CMS will use to validate ePCRs submitted by Participants; this schematron consists entirely of "Warnings" and will be treated as a set of "State" rules applicable to Participants.

   *Additional information around these customizations can be found in the **NEMSIS Data Submission – Prerecorded Webinar** available for download from the ET3 Connect Site.*

   The NEMSIS TAC has resources available for Participants on their website, and Participants are encouraged to contact the NEMSIS TAC for technical questions on the NEMSIS standard.

9. How does an ET3 Participant or supporting software vendor submit ePCR data to CMS by the required due date (the last day of the following calendar month)?

   As part of the ET3 Model onboarding process, a Participant or supporting software vendor will create an account in the CMS Enterprise Portal, and request the application programming interface (API) keys needed for secure ePCR transmission. After those API keys are issued and test transmissions are confirmed, ePCRs can be submitted using any NEMSIS-compliant ePCR software.

   Participating agencies, or their supporting software vendors, will submit ePCRs into the ET3 Model's Centralized Data Exchange (CDX) system; access to CDX is managed through the CMS Enterprise Portal. Each ePCR will be validated using the NEMSIS standard XML Schema Definition (XSD) and National Schematron schema, as well as the ET3 Model-specific "State" Schematron schema; a status code will be generated for each submission.

   Once an ePCR submission passes validation, it will be filtered, and only the elements that the ET3 Model requires will proceed to further data processing.

10. How will I know if CMS has received my ePCR data?

ET3 Participants can check the status of their ePCR submissions to the ET3 Model through the CDX Dashboard component of the ET3 application. The steps for accessing this function in CDX are detailed in Appendix E.

Participants can also reach out to their Project Officers and inquire about submission status. Email the ET3 Mailbox at ***ET3Model@cms.hhs.gov,*** *and include your Application ID in the format "ET3-0XXX" in the subject line.*

Appendices

A. ET3 Model Data Flow Diagram and Definition Table – CMMI

B. ET3 Model “State” Dataset for NEMSIS v3.4.0 – NEMSIS TAC

C. ET3 Model “State” Schematron Rules for NEMSIS v3.4 – NEMSIS TAC

D. ET3 Model Scenarios for NEMSIS v3.4.0 ePCRs – NEMSIS TAC and CMMI

E. Excerpts of User Manuals for Innovation Center (IC) Portal and CDX – CMMI

Appendix A: ET3 Model Data Flow Diagram and Definition Table – CMMI

The following graphic depicts the flows and steps associated with ET3 Data Submission.

Exhibit 1. CMS ET3 Model Data Submission Diagram (v4)

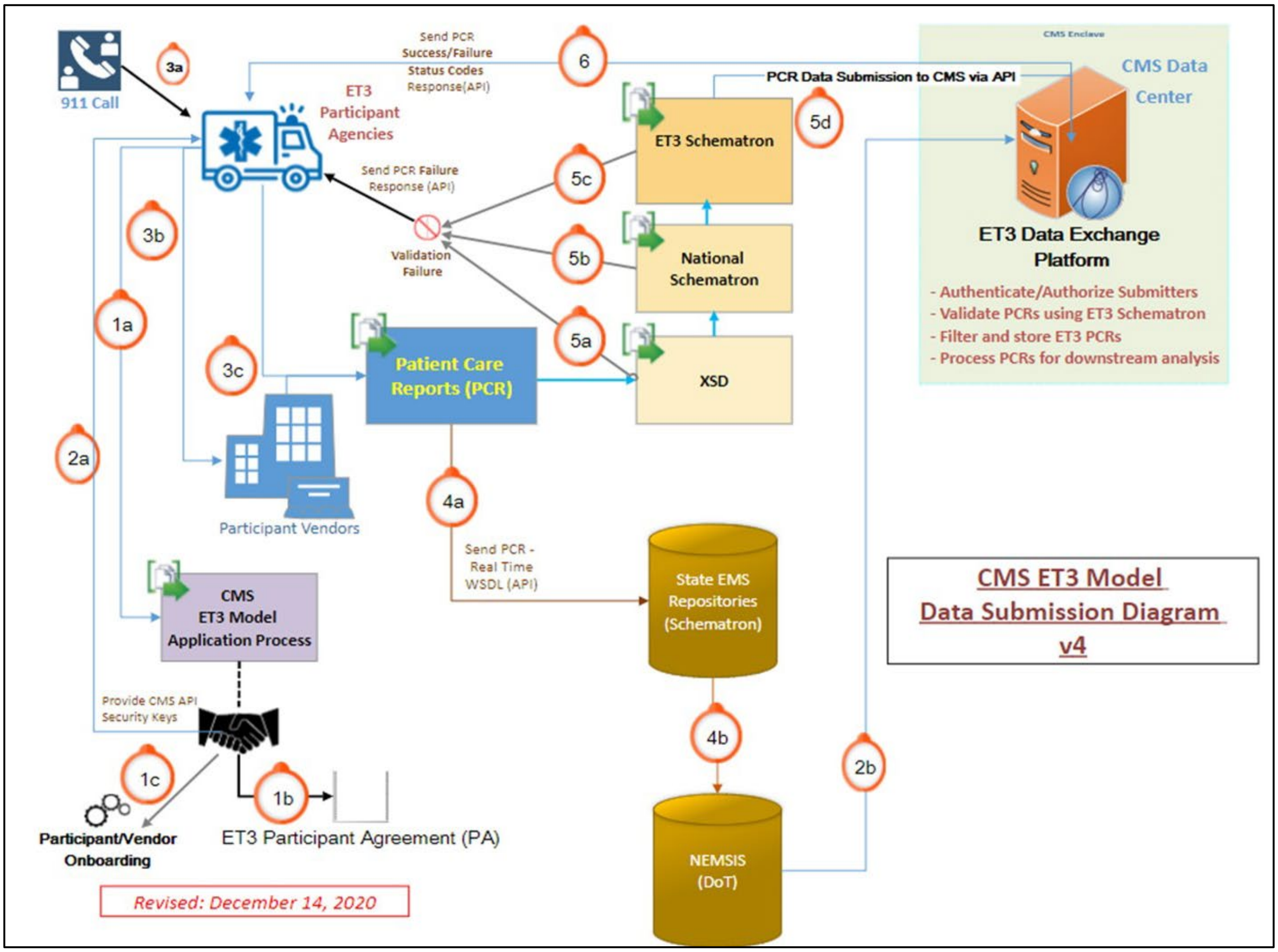

911 Call
3a
Send PCR Success/Failure Status Codes Response(API)
6
ET3 Participant Agencies
PCR Data Submission to CMS via API
CMS Enclave
CMS Data Center
5d
ET3 Schematron
Send PCR Failure Response (API)
5c
3b
Validation Failure
5b
National Schematron
ET3 Data Exchange Platform
- Authenticate/Authorize Submitters
- Validate PCRs using ET3 Schematron
- Filter and store ET3 PCRs
- Process PCRs for downstream analysis
1a
Patient Care Reports (PCR)
5a
3c
XSD
2a
Participant Vendors
4a
Send PCR - Real Time WSDL (API)
State EMS Repositories (Schematron)
CMS ET3 Model Application Process
CMS ET3 Model Data Submission Diagram v4
Provide CMS API Security Keys
4b
2b
1c
1b
Participant/Vendor Onboarding
ET3 Participant Agreement (PA)
NEMSIS (DoT)
Revised: December 14, 2020

Exhibit 2. CMS ET3 Model Data Submission Data Flow Definition Table (v3)

Ref No.	Process Type	Actor (Start)	Actor (End)	Includes	Frequency
1a	Manual	ET3 Participants Agencies	CMS ET3 Model Application Process	Application Data	Once
1b	Manual	CMS ET3 Model Application Process	ET3 Participant Agreement (PA)	CMS Approval, Application Data	Once
1c	Manual	CMS ET3 Model Team	ET3 Participant/Vendor Onboarding (PA)	ET3 Webinar, User Guidance, Security Keys, etc.	Once
2a	Online	CMS ET3 Model Team	ET3 Participant Agencies & Vendors	ET3 Webinar, User Guidance, Security Keys, etc.	Once
2b	File Transfer	NEMSIS TAC (DOT)	ET3 Data Exchange Platform	Participant Demographic Data	4 times per year
3a	911 Call	911 Call Center	ET3 Participant Agencies	Incident Details	Continuous
3b	Data Submission	ET3 Participant Agencies	ET3 Participant Vendors	Patient Care Information	Continuous
3c	Data Submission	ET3 Participant Agencies/ Vendors	Electronic Patient Care Report (PCR) records	Patient Care Reports (PCR)	Continuous
4a	State Data Submission & Validation	Patient Care Reports (PCR)	State EMS Repositories	PCR Data & State Schematron	Continuous
4b	National Data Submission & Validation	Patient Care Reports (PCR)	NEMSIS National Repository	PCR Data & National Schematron	Continuous
5a	ET3 Data Validation	XML Schema Definition (XSD)	Validation Failure	PCR Data & XSD	Only when Validation fails
5b	ET3 Data Validation	National Schematron	Validation Failure	PCR Data National Schematron	Only when Validation fails
5c	ET3 Data Validation	ET3 Schematron	Validation Failure	PCR Data and ET3 Schematron	Only when Validation fails
5d	Data Submission (Successful)	ET3 Schematron	ET3 Data Exchange Platform	PCR Data sent to CMS via NEMSIS API	Continuous
6	Data Submission Response (Success or Fail)	ET3 Data Exchange Platform	ET3 Participant Agencies/ Vendors	ET3 Validation Response from ET3 Data Exchange Platform	Continuous

Starting in the lower left corner of the diagram, prospective Participants first applied for entry into the ET3 Model using the ET3 Model Application Process (see Flow 1a). This was a manual process, which resulted in the transfer of Applicant data to CMMI.

ET3 Participants later signed Participant Agreements, which then permitted participation in ET3 Model Onboarding activities (see Flows 1b & 1c). Additionally, Participants could then request access to the ET3 Model system by registering through the CMS Enterprise Portal (https://portal.cms.gov).

Concurrent with ET3 Model Onboarding activities, the NEMSIS TAC generates a Department of Transportation (DoT) file containing Demographic Data for all of the ET3 Model's participating EMS agencies (see Flow 2b).

Once a 911 call is initiated, a participating ambulance supplier or provider responds to the incident location and provides EMS to any affected patient(s) or Medicare beneficiary(ies). While treatment activities are the highest priority, the collection of patient data begins.

Using a software vendor's product, EMS personnel collect ePCR data and the data are formatted using the NEMSIS standard prior to transmission (see Flows 3b & 3c). Once the complete ePCR data are collected, the ePCR software vendor will send the ePCR data to the state in which the Participant is licensed to provide EMS (see Flow 4a). Each state participating in the NEMSIS standard sends a subset of ePCR data to the national NEMSIS Data Repository (see Flow 4b).

After successfully transmitting ePCR data to the state, the ePCR software vendor will then send the ePCR data to the ET3 Model (see Flow 5a). The validation process is performed in three steps, starting with the XSD, then the National Schematron schema, and finally the ET3 Model "State" Schematron schema validation. If a validation failure occurs at any point in the three-step validation process, then the ET3 Model-bound data are not sent further through CMS systems (see Flows 5a, 5b, & 5c). Once a successful validation process occurs, ePCR records continue through systems for further processing (see Flows 5d). Either a SUCCESS or FAILURE response report will be sent back to whomever submits the ePCR data (see Flow 6a).

Once accepted, the ePCR data are filtered and only the required ET3 Model data submission elements (see Appendix B) are stored and processed for downstream data analyses.

Appendix B: ET3 Model “State” Dataset for NEMSIS v3.4.0 – NEMSIS TAC

The ET3 Model “State” Dataset for NEMSIS v3.4.0 can be found online at https://stash.utahdcc.org/stash/projects/NES/repos/et3-project/raw/Resources/ET3_StateDataSet.pdf?at=refs%2Fheads%2Frelease-3.4.0

Appendix C: ET3 Model “State” Dataset Schematron Rules for NEMSIS v3.4 – NEMSIS TAC

The ET3 Model “State” Dataset Schematron Rules for NEMSIS v3.4 can be found online at https://stash.utahdcc.org/stash/projects/NES/repos/et3-project/raw/Schematron/ET3_EMSDataSet.sch.pdf?at=refs%2Fheads%2Frelease-3.4.0

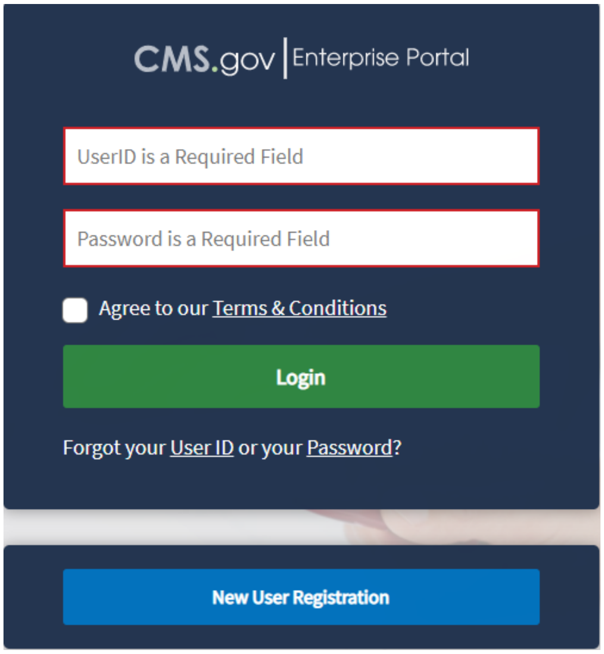
Appendix D: ET3 Model Scenarios for NEMSIS v3.4.0 ePCRs – NEMSIS TAC and CMMI

The ET3 Model Scenarios for NEMSIS v3.4.0 ePCRs can be found online at https://stash.utahdcc.org/stash/projects/NES/repos/et3-project/raw/Resources/ET3_CustomDispositions.pdf?at=refs%2Fheads%2Frelease-3.4.0.

Appendix E: Excerpts of User Manuals for Innovation Center (IC) Portal and CDX – CMMI

Before accessing the CMS ePortal (https://portal.cms.gov/), you will need to create a user ID and password by completing the Enterprise Identify Management (EIDM) user registration process.

Go to https://portal.cms.gov/ and click on **New User Registration**.



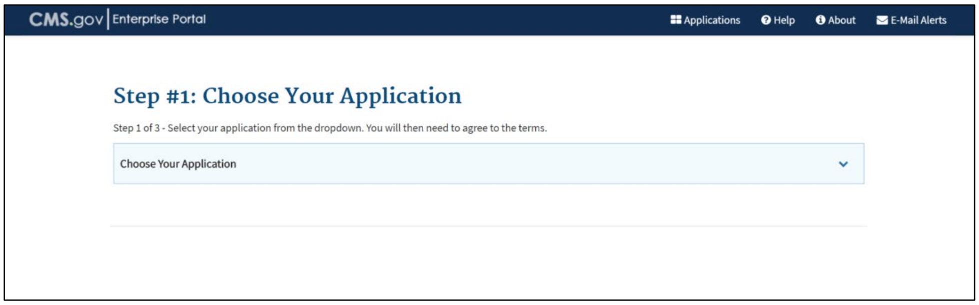
UserID is a Required Field

Password is a Required Field

□ Agree to our Terms & Conditions

Forgot your User ID or your Password?

1. On the **Choose Your Application** page, select your application from the **Choose Your Application** drop-down.

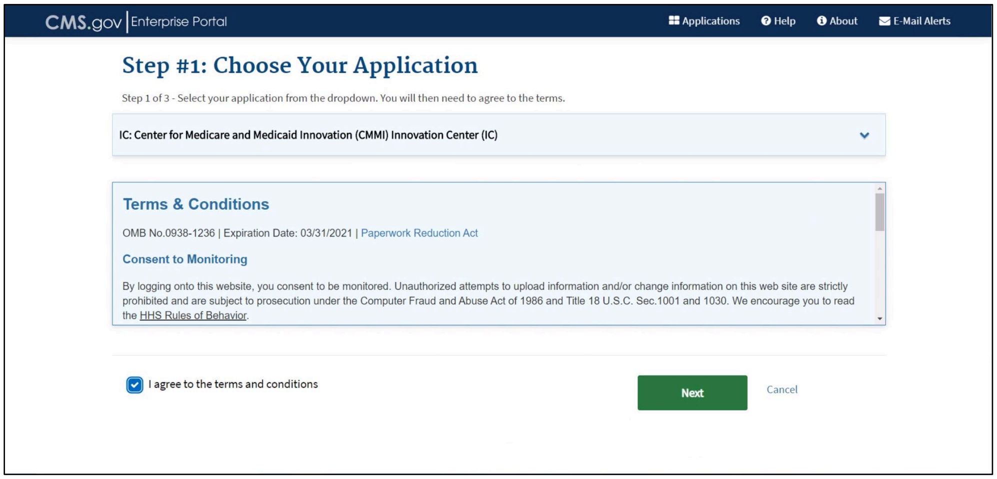


Step #1: Choose Your Application

Step 1 of 3 - Select your application from the dropdown. You will then need to agree to the terms.

Choose Your Application

2. Select **IC: CMS Innovation Center (IC)** and acknowledge you have read the terms and conditions by clicking the box indicating **"I agree to the terms and conditions."**



Step #1: Choose Your Application

Step 1 of 3 - Select your application from the dropdown. You will then need to agree to the terms.

IC: Center for Medicare and Medicaid Innovation (CMMI) Innovation Center (IC)

Terms & Conditions

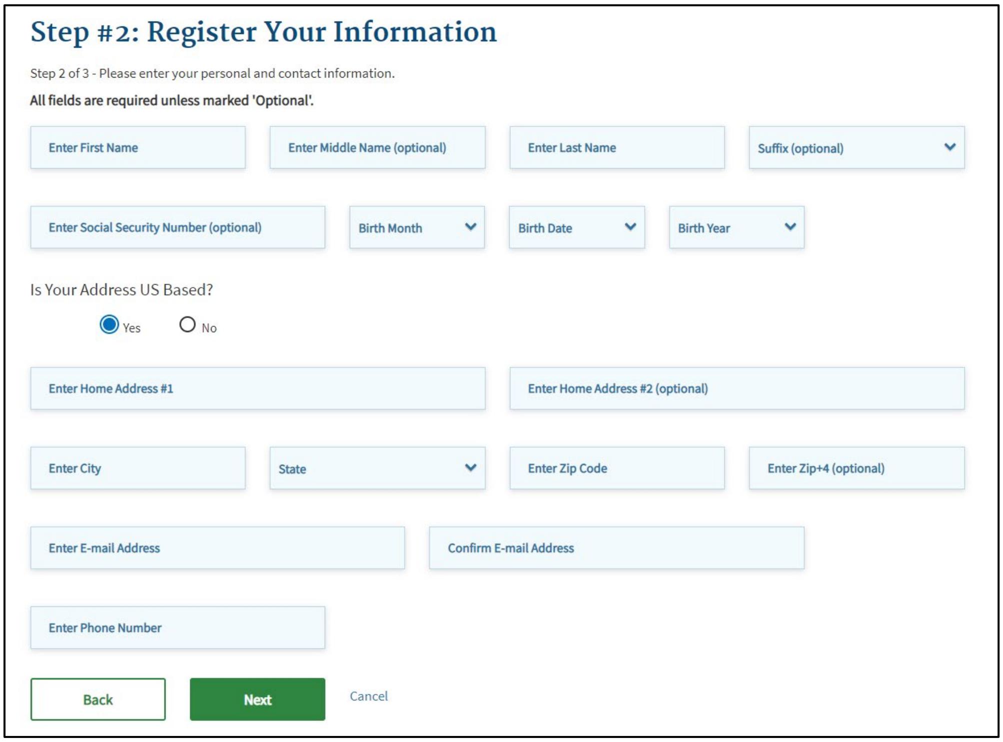
OMB No.0938-1236 | Expiration Date: 03/31/2021 | Paperwork Reduction Act

Consent to Monitoring

By logging onto this website, you consent to be monitored. Unauthorized attempts to upload information and/or change information on this web site are strictly prohibited and are subject to prosecution under the Computer Fraud and Abuse Act of 1986 and Title 18 U.S.C. Sec.1001 and 1030. We encourage you to read the HHS Rules of Behavior.

☑ I agree to the terms and conditions

3. On the **Register Your Information** page, fill out the page with your personal information.


Step #2: Register Your Information

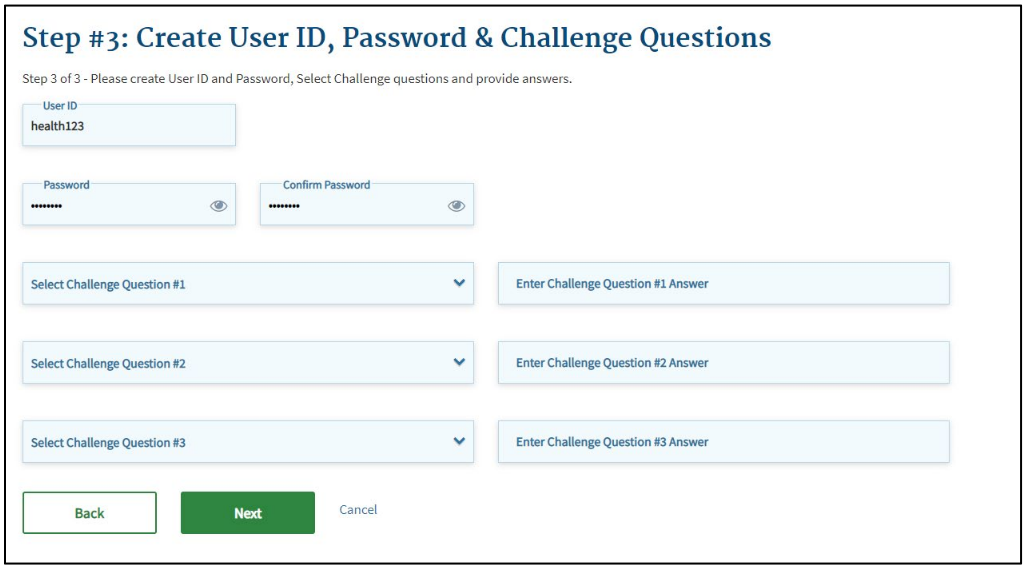
Step 2 of 3 - Please enter your personal and contact information.

All fields are required unless marked 'Optional'.

Is Your Address US Based?

● Yes ○ No

4. On the **Create User ID, Password & Challenge Questions** page, fill out the page with your chosen CMS access credentials.



Step #3: Create User ID, Password & Challenge Questions

Step 3 of 3 - Please create User ID and Password, Select Challenge questions and provide answers.

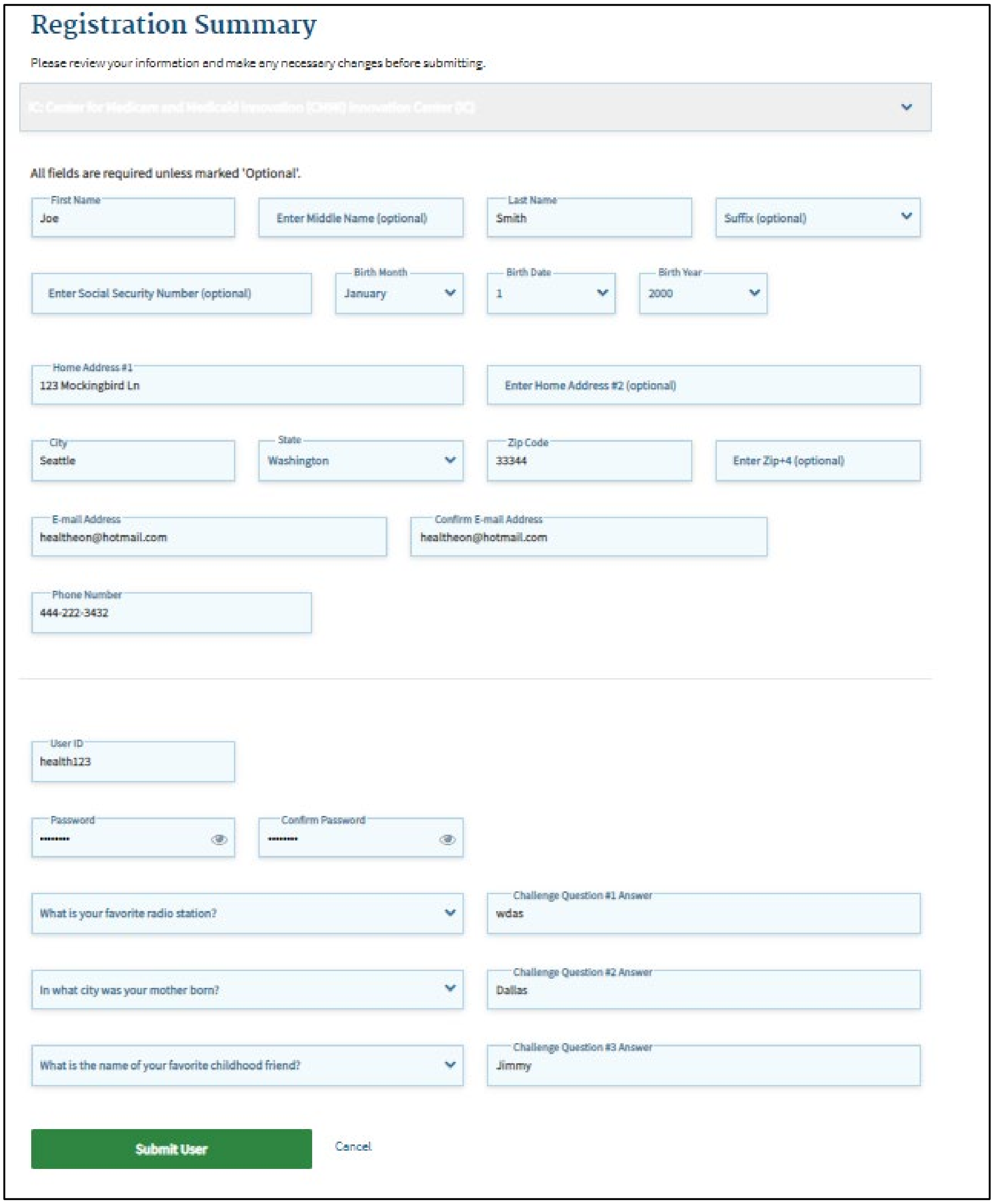
User ID: health123

Password: ••••••••

Confirm Password: ••••••••

Select Challenge Question #1
Enter Challenge Question #1 Answer
Select Challenge Question #2
Enter Challenge Question #2 Answer
Select Challenge Question #3
Enter Challenge Question #3 Answer
Back
Next
Cancel

5. Review the **Registration Summary** page to ensure your choices and personal information are accurate.



Registration Summary

Please review your information and make any necessary changes before submitting.

IC: Center for Medicare and Medicaid Innovation (CMMI) Innovation Center (IC)

All fields are required unless marked 'Optional'.

First Name: Joe
Enter Middle Name (optional)
Last Name: Smith
Suffix (optional)

Enter Social Security Number (optional)
Birth Month: January
Birth Date: 1
Birth Year: 2000

Home Address #1: 123 Mockingbird Ln
Enter Home Address #2 (optional)

City: Seattle
State: Washington
Zip Code: 33344
Enter Zip+4 (optional)

E-mail Address: healtheon@hotmail.com
Confirm E-mail Address: healtheon@hotmail.com

Phone Number: 444-222-3432

User ID: health123

Password: ••••••••
Confirm Password: ••••••••

What is your favorite radio station?
Challenge Question #1 Answer: wdas

In what city was your mother born?
Challenge Question #2 Answer: Dallas

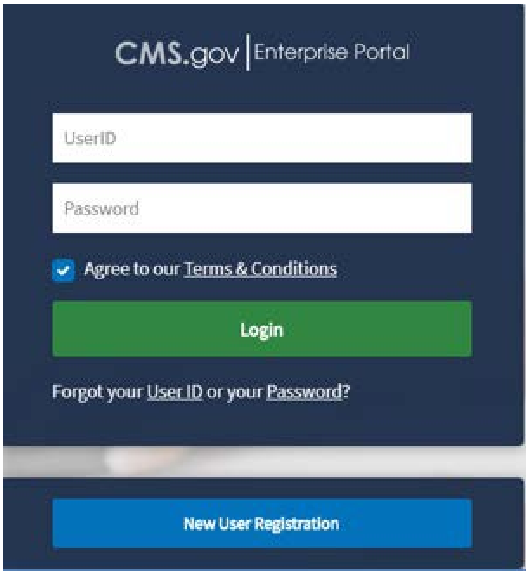
What is the name of your favorite childhood friend?
Challenge Question #3 Answer: Jimmy

6. Click on the “Submit User” button located at the bottom of the page.

Once you have successfully completed EIDM registration, you may log in to the ePortal and request an Innovation Center (IC) Application role. To request an IC Application role, you must successfully complete the Remote Identity Proofing (RIDP) process and register your Multi-Factor Authentication (MFA) device. Once your IC Application user role request is approved, you may request access to the CMMI CDX Application.

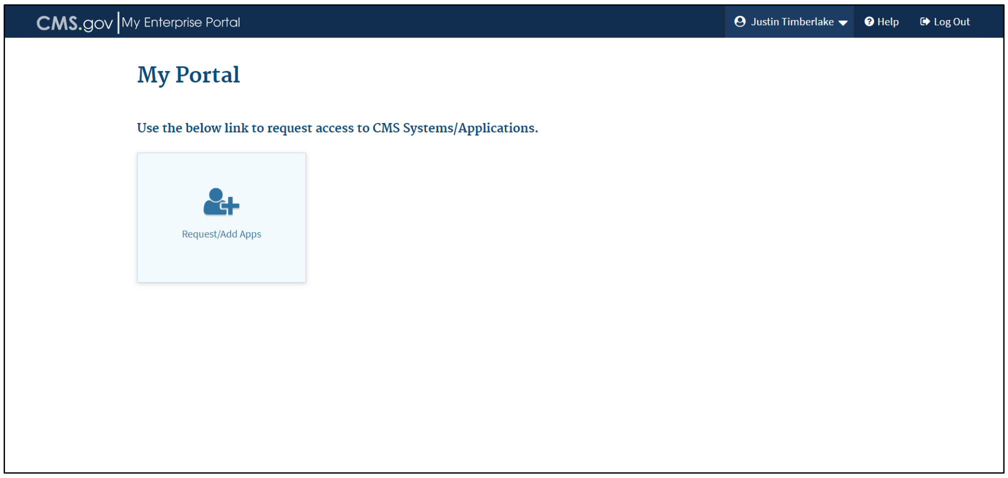
To request access, please complete the following steps.

1. Go to https://portal.cms.gov/ and log in using your credentials and security code.


CMS.gov | Enterprise Portal
UserID
Password
☑ Agree to our Terms & Conditions
Login
Forgot your User ID or your Password?
New User Registration

2. Access the catalog by:

- Selecting the **My Access** option from the Welcome drop-down list in the top navigation bar, or
- Clicking the **Request/Add Apps** tile on the **My Portal** page.

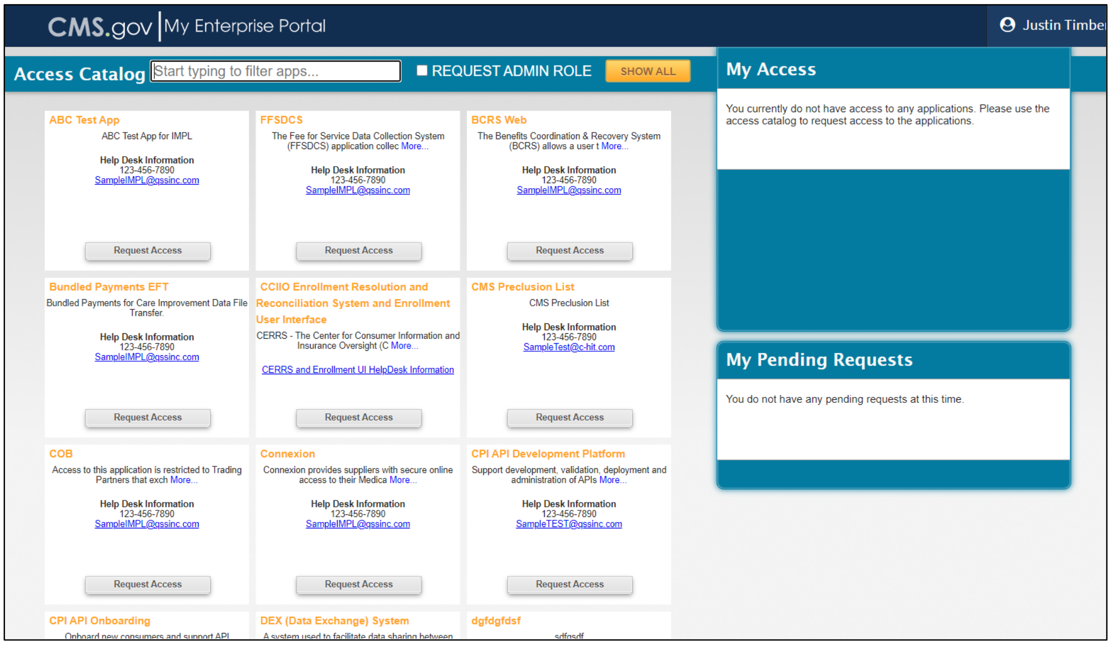


My Portal

Use the below link to request access to CMS Systems/Applications.

3. A set of CMS systems will appear in tiles:

- Look for the system tile called "Innovation Center (IC), or
- Enter **"IC"** into the filter field to find the tile.


CMS.gov | My Enterprise Portal

Justin Timbe

Access Catalog Start typing to filter apps... □ REQUEST ADMIN ROLE SHOW ALL

ABC Test App
ABC Test App for IMPL
Help Desk Information
123-456-7890
SampleIMPL@qssinc.com
Request Access

FFSDCS
The Fee for Service Data Collection System (FFSDCS) application collec More...
Help Desk Information
123-456-7890
SampleIMPL@qssinc.com
Request Access

BCRS Web
The Benefits Coordination & Recovery System (BCRS) allows a user t More...
Help Desk Information
123-456-7890
SampleIMPL@qssinc.com
Request Access

Bundled Payments EFT
Bundled Payments for Care Improvement Data File Transfer.
Help Desk Information
123-456-7890
SampleIMPL@qssinc.com
Request Access

CCIIO Enrollment Resolution and Reconciliation System and Enrollment User Interface
CERRS - The Center for Consumer Information and Insurance Oversight (C More...
CERRS and Enrollment UI HelpDesk Information
Request Access

CMS Preclusion List
CMS Preclusion List
Help Desk Information
123-456-7890
SampleTest@c-hit.com
Request Access

COB
Access to this application is restricted to Trading Partners that exch More...
Help Desk Information
123-456-7890
SampleIMPL@qssinc.com
Request Access

Connexion
Connexion provides suppliers with secure online access to their Medica More...
Help Desk Information
123-456-7890
SampleIMPL@qssinc.com
Request Access

CPI API Development Platform
Support development, validation, deployment and administration of APIs More...
Help Desk Information
123-456-7890
SampleTEST@qssinc.com
Request Access

CPI API Onboarding
Onboard new consumers and support API

DEX (Data Exchange) System
A system used to facilitate data sharing between

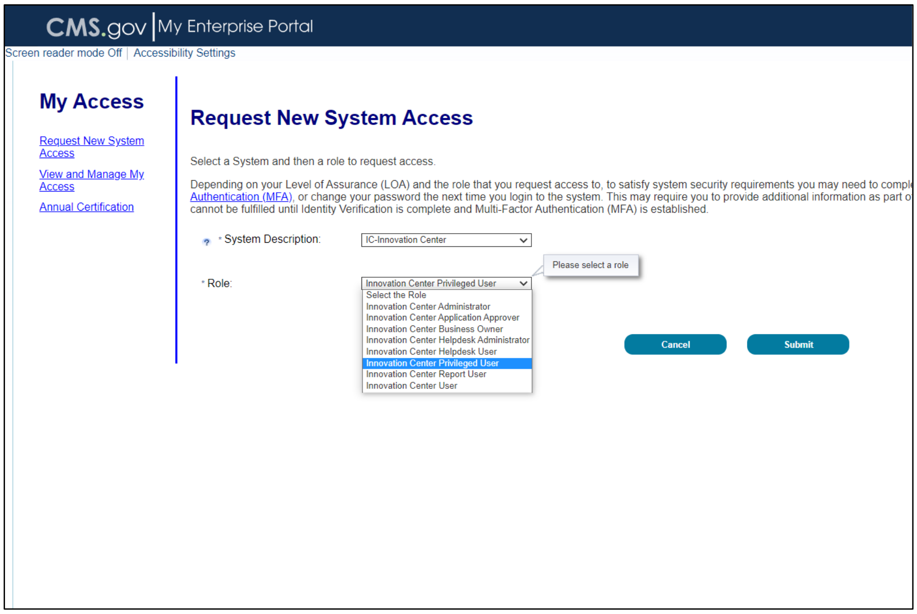
dgfdgfdsf
sdfasdf

My Access
You currently do not have access to any applications. Please use the access catalog to request access to the applications.

My Pending Requests
You do not have any pending requests at this time.

Click on the **Request Access** button for the IC tile.

4. Select **Innovation Center Privileged User** from the **Role** drop down menu.


CMS.gov | My Enterprise Portal

Screen reader mode Off | Accessibility Settings

My Access

Request New System Access
View and Manage My Access
Annual Certification

Request New System Access

Select a System and then a role to request access.

Depending on your Level of Assurance (LOA) and the role that you request access to, to satisfy system security requirements you may need to compl Authentication (MFA), or change your password the next time you login to the system. This may require you to provide additional information as part o cannot be fulfilled until Identity Verification is complete and Multi-Factor Authentication (MFA) is established.

* System Description: IC-Innovation Center

* Role: Innovation Center Privileged User

Please select a role

Select the Role
Innovation Center Administrator
Innovation Center Application Approver
Innovation Center Business Owner
Innovation Center Helpdesk Administrator
Innovation Center Helpdesk User
Innovation Center Privileged User
Innovation Center Report User
Innovation Center User
Cancel
Submit

Click the **Submit** button.

Remote Identity Proofing (RIDP)

CMS uses the **Experian identity verification system** (Experian) to remotely perform identity proofing. Experian is used by CMS to confirm your identity when you need to access a protected CMS Computer System.

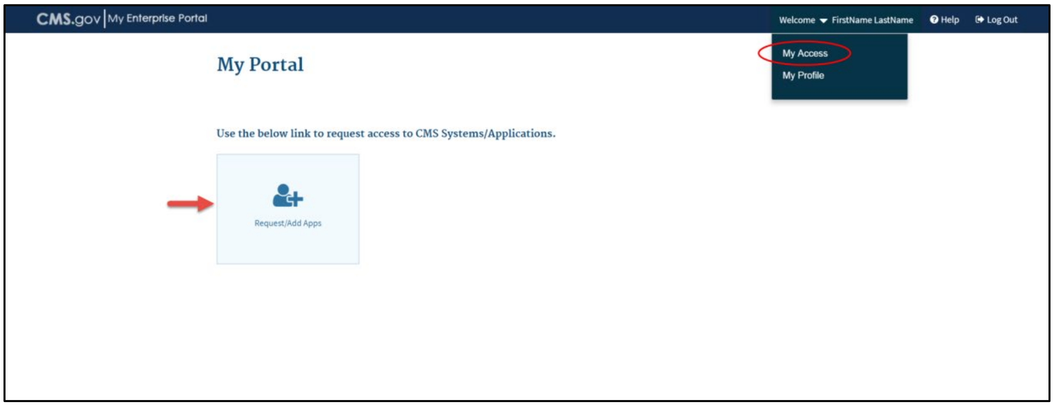
The following data elements are requested from users:

- Full Legal Name
- Social Security Number (SSN)
- Date of Birth
- Current Residential Address
- Personal Telephone Number

CMS does not store your personal information; CMS only passes it to Experian to help confirm your identity. Your SSN will be validated with Experian only for the purpose of verifying your identity.

To complete the RIDP process, please complete the following steps.

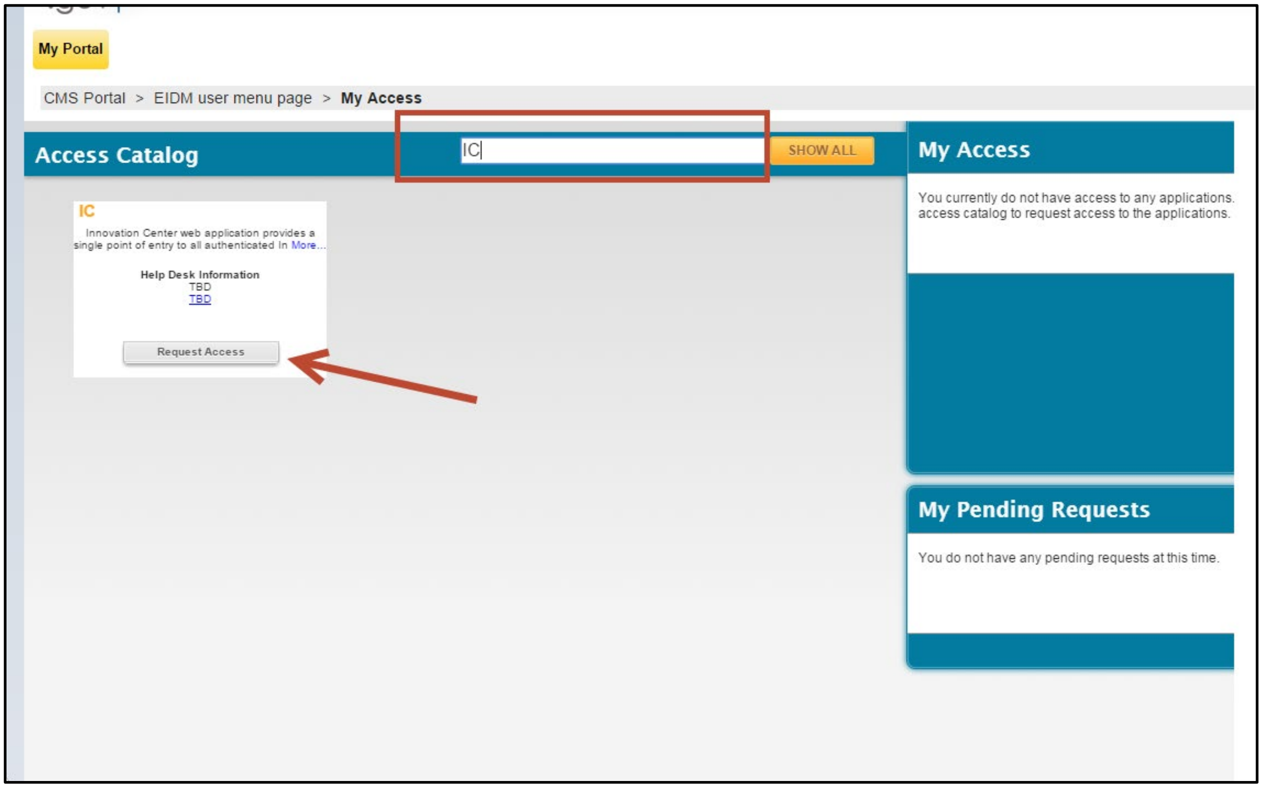
1. On the CMS Enterprise Portal Main Page, click on **Request/Add Apps tile** on the My Portal page or My Access option from the Welcome drop-down list.



My Portal

Use the below link to request access to CMS Systems/Applications.

2. The application Access Catalog displays all CMS applications that use EIDM services. Type **"IC"** in the search box and press **"Enter"** to find the IC application.



IC

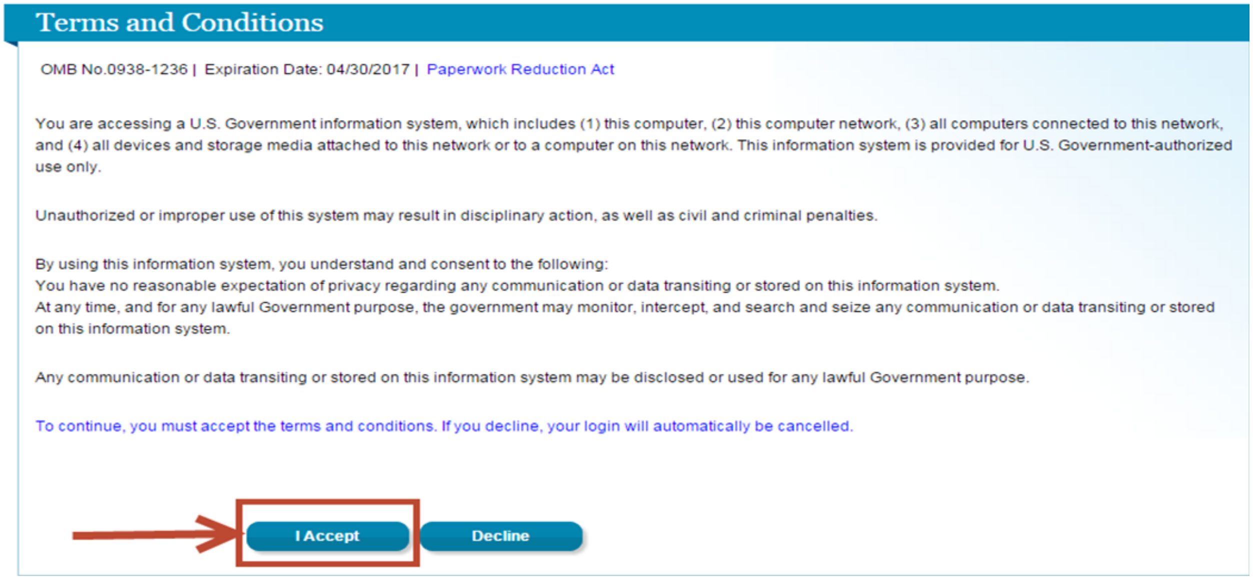
Innovation Center web application provides a single point of entry to all authenticated In More...

Help Desk Information
TBD
TBD

You currently do not have access to any applications. access catalog to request access to the applications.

You do not have any pending requests at this time.

3. Read and accept or decline the "Terms and Conditions" by clicking the appropriate I **Accept** or **Decline** option.



OMB No.0938-1236 | Expiration Date: 04/30/2017 | Paperwork Reduction Act

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

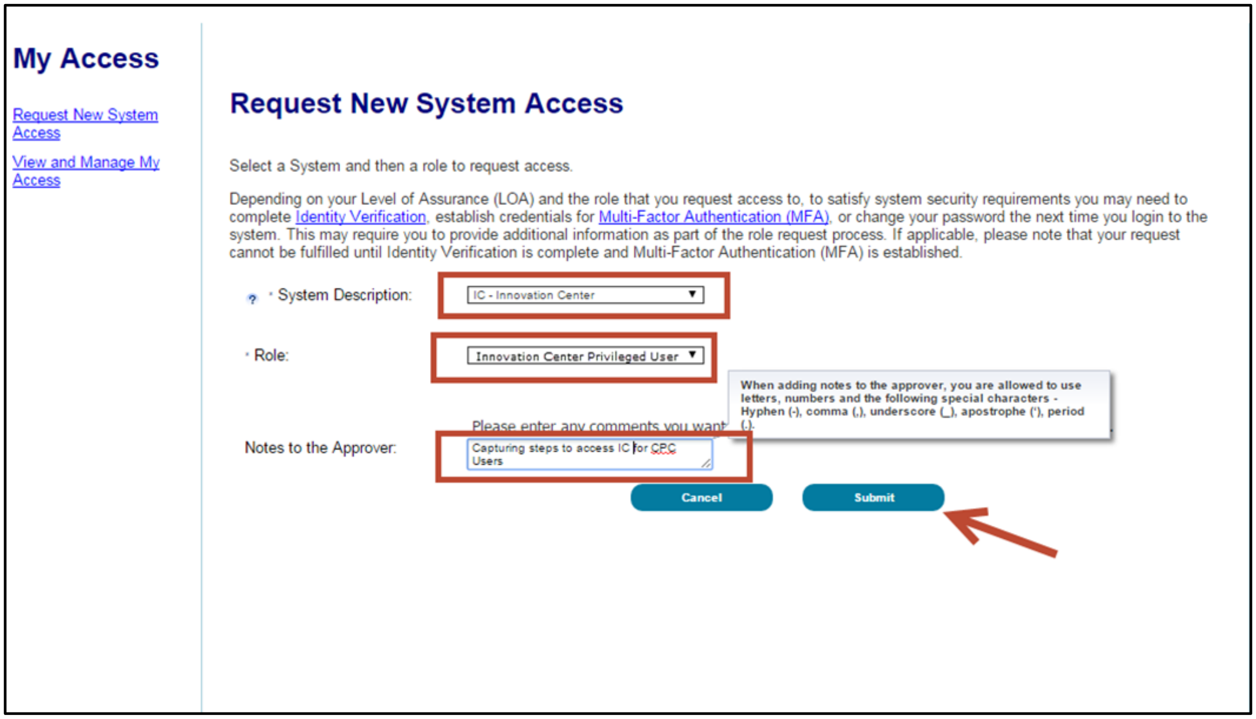
By using this information system, you understand and consent to the following:
You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system.
At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.

Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.

To continue, you must accept the terms and conditions. If you decline, your login will automatically be cancelled.

Depending on your Level of Assurance (LOA) and the role that you request access to, you may need to complete the Identity Verification; establish credentials for MFA, and change your password the next time you log in to the system.

1. Fill out the initial "**Request New System Access**" form.



My Access

Request New System Access

View and Manage My Access

Request New System Access

Select a System and then a role to request access.

Depending on your Level of Assurance (LOA) and the role that you request access to, to satisfy system security requirements you may need to complete Identity Verification, establish credentials for Multi-Factor Authentication (MFA), or change your password the next time you login to the system. This may require you to provide additional information as part of the role request process. If applicable, please note that your request cannot be fulfilled until Identity Verification is complete and Multi-Factor Authentication (MFA) is established.

* System Description: IC - Innovation Center ▼

* Role: Innovation Center Privileged User ▼

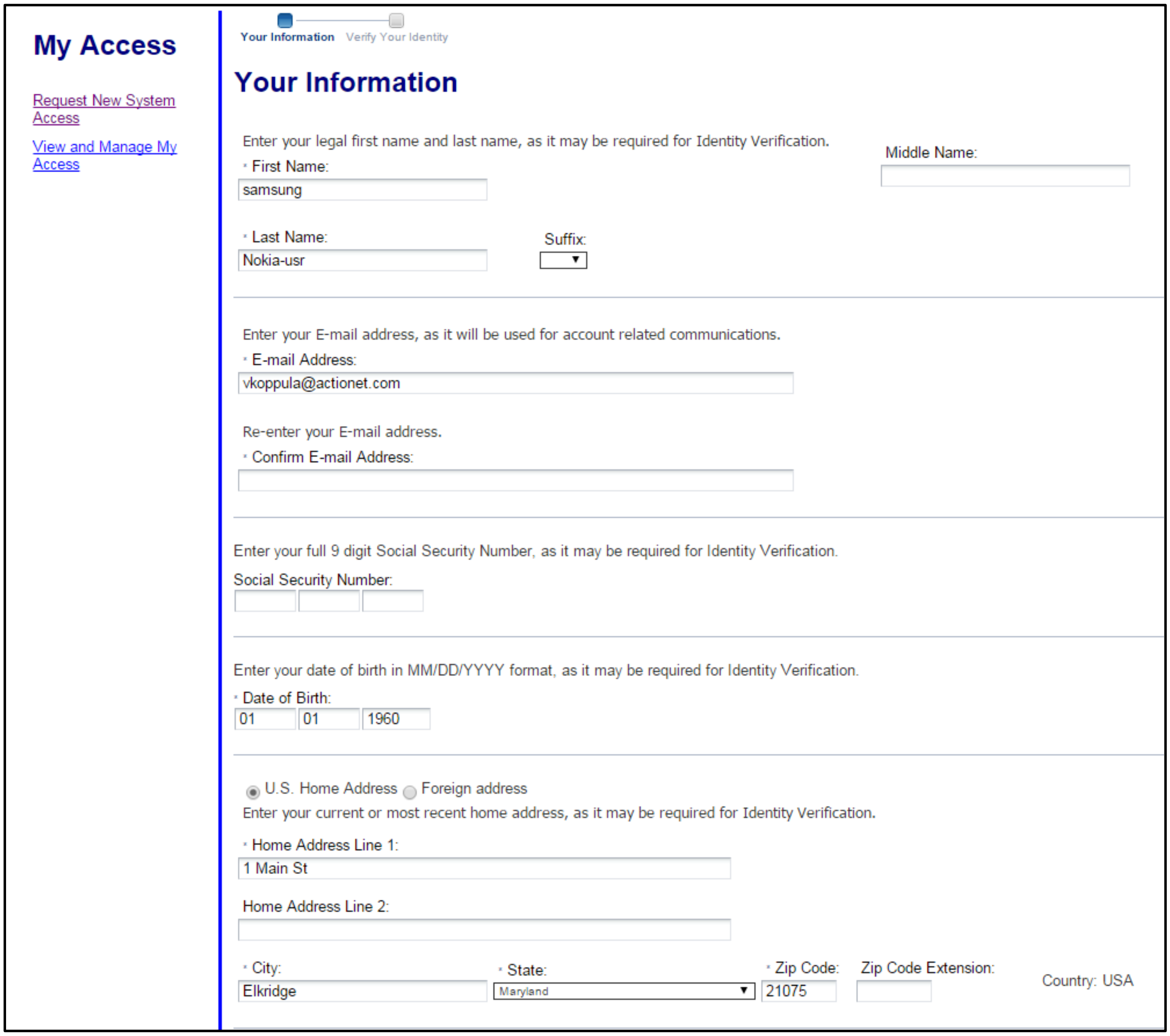
Please enter any comments you want

When adding notes to the approver, you are allowed to use letters, numbers and the following special characters - Hyphen (-), comma (,), underscore (_), apostrophe ('), period (.).

Notes to the Approver: Capturing steps to access IC for CPC Users

Click **Submit.**

2. Verify and confirm that your personal information on the “Your Information” screen is correct and click the **“Next”** button.



Your Information

Enter your legal first name and last name, as it may be required for Identity Verification.

First Name: samsung

Middle Name:

Last Name: Nokia-usr

Suffix:

Enter your E-mail address, as it will be used for account related communications.

E-mail Address: vkoppula@actionet.com

Re-enter your E-mail address.

Confirm E-mail Address:

Enter your full 9 digit Social Security Number, as it may be required for Identity Verification.

Social Security Number:

Enter your date of birth in MM/DD/YYYY format, as it may be required for Identity Verification.

Date of Birth: 01 01 1960

● U.S. Home Address ○ Foreign address

Enter your current or most recent home address, as it may be required for Identity Verification.

Home Address Line 1: 1 Main St

Home Address Line 2:

City: Elkridge

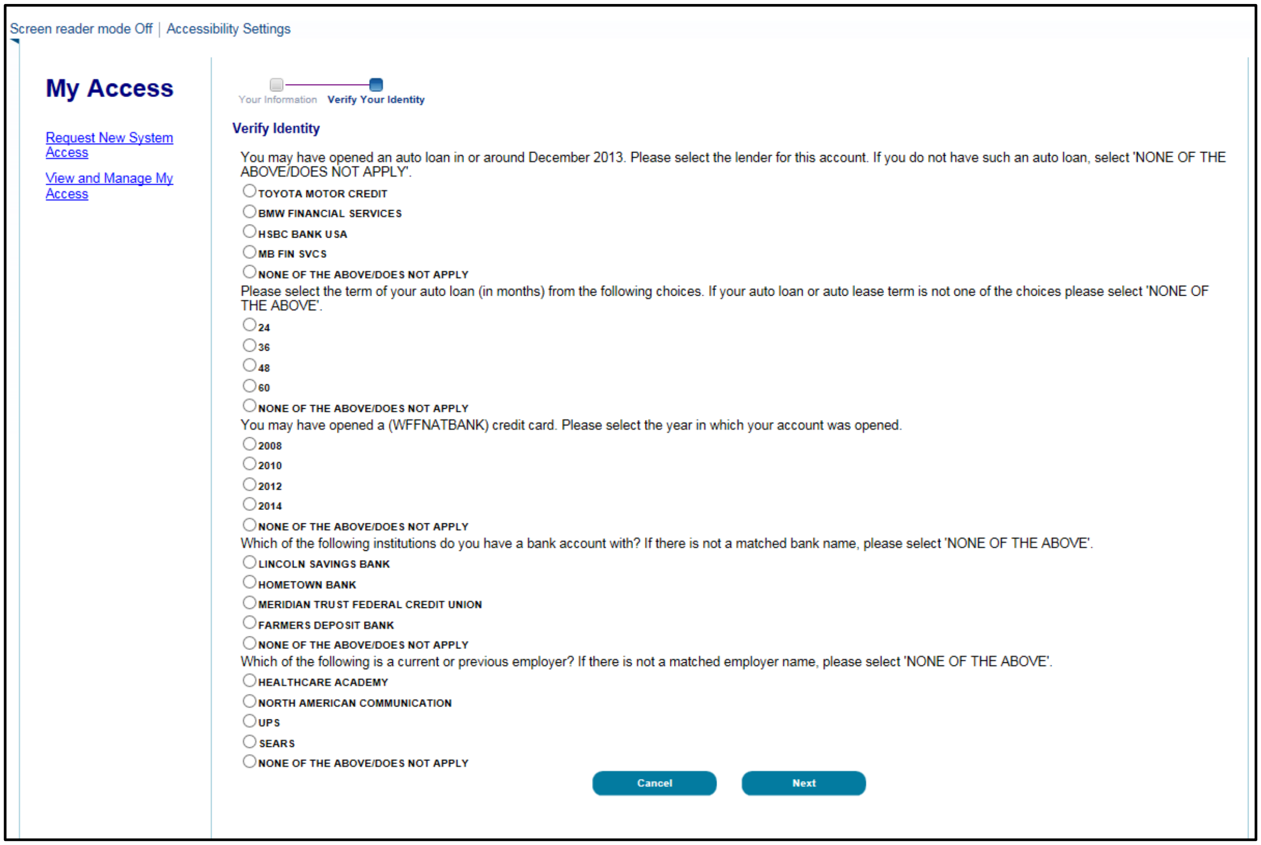
State: Maryland

Zip Code: 21075

Zip Code Extension:

Country: USA

3. Enter the required information for MFA on the “Verify Identity” screen and click the **“Next”** button.



Screen reader mode Off | Accessibility Settings

My Access

Request New System Access

View and Manage My Access

Verify Identity

You may have opened an auto loan in or around December 2013. Please select the lender for this account. If you do not have such an auto loan, select 'NONE OF THE ABOVE/DOES NOT APPLY'.

○ TOYOTA MOTOR CREDIT
○ BMW FINANCIAL SERVICES
○ HSBC BANK USA
○ MB FIN SVCS
○ NONE OF THE ABOVE/DOES NOT APPLY

Please select the term of your auto loan (in months) from the following choices. If your auto loan or auto lease term is not one of the choices please select 'NONE OF THE ABOVE'.

○ 24
○ 36
○ 48
○ 60
○ NONE OF THE ABOVE/DOES NOT APPLY

You may have opened a (WFFNATBANK) credit card. Please select the year in which your account was opened.

○ 2008
○ 2010
○ 2012
○ 2014
○ NONE OF THE ABOVE/DOES NOT APPLY

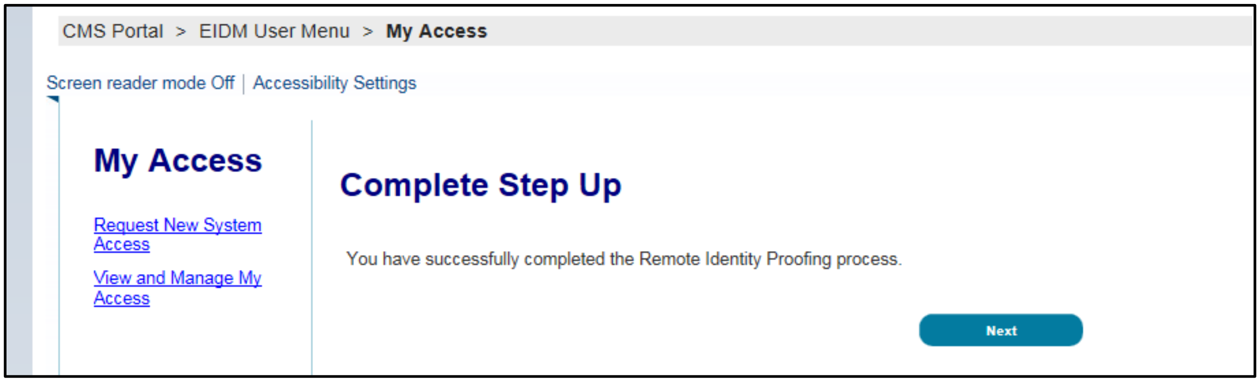
Which of the following institutions do you have a bank account with? If there is not a matched bank name, please select 'NONE OF THE ABOVE'.

○ LINCOLN SAVINGS BANK
○ HOMETOWN BANK
○ MERIDIAN TRUST FEDERAL CREDIT UNION
○ FARMERS DEPOSIT BANK
○ NONE OF THE ABOVE/DOES NOT APPLY

Which of the following is a current or previous employer? If there is not a matched employer name, please select 'NONE OF THE ABOVE'.

○ HEALTHCARE ACADEMY
○ NORTH AMERICAN COMMUNICATION
○ UPS
○ SEARS
○ NONE OF THE ABOVE/DOES NOT APPLY

4. Click the **“Next”** button on the “Complete Set Up” screen.



CMS Portal > EIDM User Menu > My Access

Screen reader mode Off | Accessibility Settings

My Access

Request New System Access

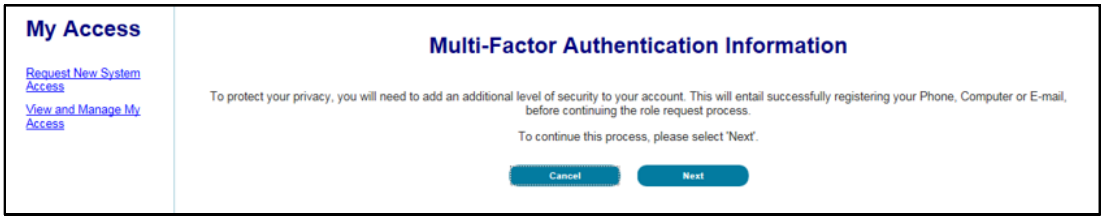
View and Manage My Access

Complete Step Up

You have successfully completed the Remote Identity Proofing process.

MFA Information. You will need to add an additional level of security to your user account.

1. Click the **“Next”** button to continue the MFA process.

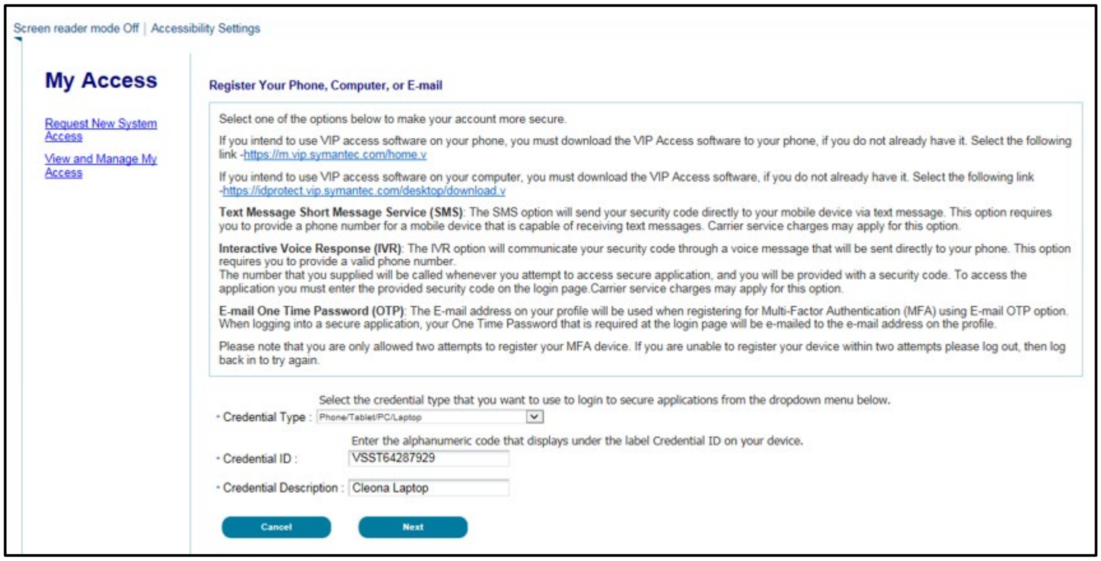


Multi-Factor Authentication Information

To protect your privacy, you will need to add an additional level of security to your account. This will entail successfully registering your Phone, Computer or E-mail, before continuing the role request process.

To continue this process, please select 'Next'.

2. You have the option to receive the MFA security code via Smart Phone/Computer, Short Message Service (SMS), Interactive Voice Response (IVR), or email by providing the applicable information on the “Register Your Phone, Computer, or Email” screen.



Screen reader mode Off | Accessibility Settings
My Access
Request New System Access
View and Manage My Access

Register Your Phone, Computer, or E-mail

Select one of the options below to make your account more secure.

If you intend to use VIP access software on your phone, you must download the VIP Access software to your phone, if you do not already have it. Select the following link -https://m.vip.symantec.com/home.v

If you intend to use VIP access software on your computer, you must download the VIP Access software, if you do not already have it. Select the following link -https://idprotect.vip.symantec.com/desktop/download.v

Text Message Short Message Service (SMS): The SMS option will send your security code directly to your mobile device via text message. This option requires you to provide a phone number for a mobile device that is capable of receiving text messages. Carrier service charges may apply for this option.

Interactive Voice Response (IVR): The IVR option will communicate your security code through a voice message that will be sent directly to your phone. This option requires you to provide a valid phone number.
The number that you supplied will be called whenever you attempt to access secure application, and you will be provided with a security code. To access the application you must enter the provided security code on the login page.Carrier service charges may apply for this option.

E-mail One Time Password (OTP): The E-mail address on your profile will be used when registering for Multi-Factor Authentication (MFA) using E-mail OTP option. When logging into a secure application, your One Time Password that is required at the login page will be e-mailed to the e-mail address on the profile.

Please note that you are only allowed two attempts to register your MFA device. If you are unable to register your device within two attempts please log out, then log back in to try again.

Select the credential type that you want to use to login to secure applications from the dropdown menu below.
- Credential Type : Phone/Tablet/PC/Laptop

Enter the alphanumeric code that displays under the label Credential ID on your device.
- Credential ID : VSST64287929
- Credential Description : Cleona Laptop

SMART PHONE / COMPUTER: You will need to download the Symantec VIP Access software on your smart phone or computer. This installation will require you to navigate to another screen, then return to the MFA screen to complete the process.

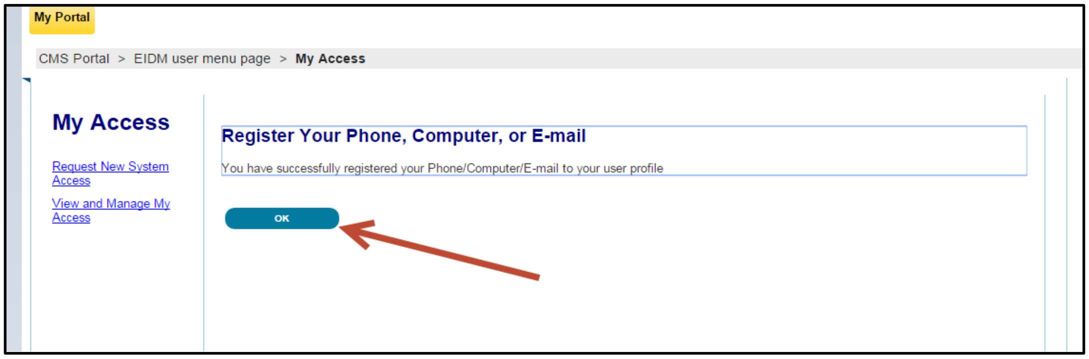
Once VIP Access has been downloaded/installed successfully, launch the application. Enter the alphanumeric Credential ID that is generated by the VIP Access client, credential description, and click Next.

TEXT MESSAGE (SMS): Use the SMS option to have the Security Code sent by text to your mobile phone. Enter a valid phone number capable of receive text messages, credential description, and click Next.

INTERACTIVE VOICE RESPONSE (IVR): Use the IVR option to receive a voice message containing the Security Code. Enter a valid phone number and (optional) phone extension, credential description, and click Next.

E-MAIL: Use the email option to receive an email containing the Security Code required to login. The system uses the email address in your user profile. Click Next.

3. Complete registration by clicking **"OK."**


My Portal
CMS Portal > EIDM user menu page > My Access
My Access
Request New System Access
View and Manage My Access
OK

Register Your Phone, Computer, or E-mail

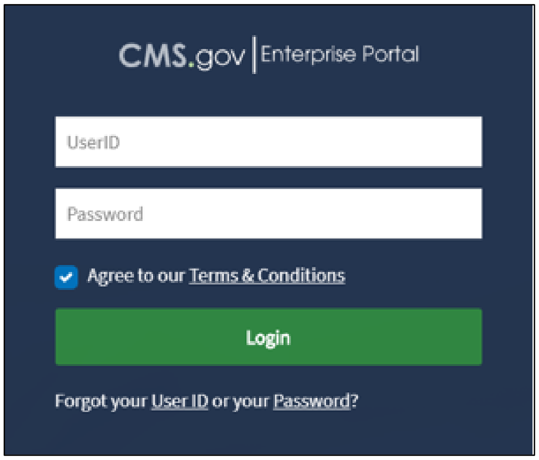
You have successfully registered your Phone/Computer/E-mail to your user profile

You now have finished the RIDP and MFA process.

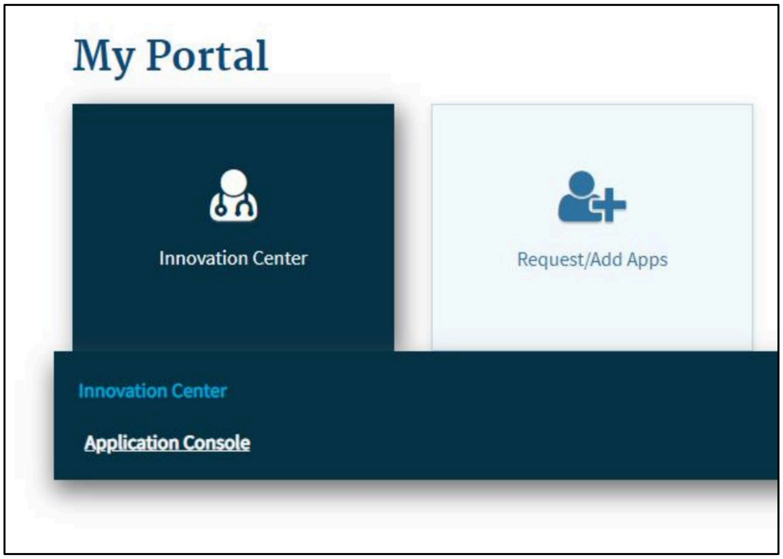
SUBMIT ROLE REQUEST FOR ACCESSING CENTRALIZED DATA EXCHANGE (CDX) APPLICATION

To submit a role request for accessing the CDX application, please complete the following steps.

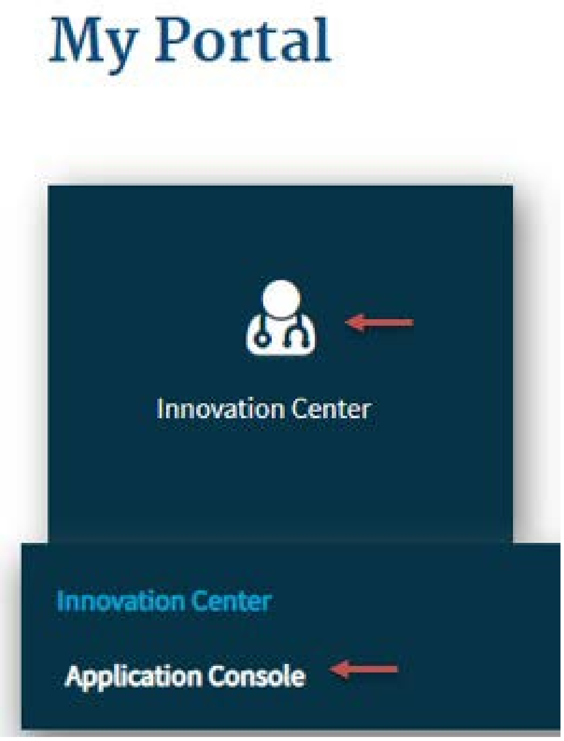
1. Go to https://portal.cms.gov/ and log in using your credentials and security code.


CMS.gov | Enterprise Portal
UserID
Password
Agree to our Terms & Conditions
Login
Forgot your User ID or your Password?

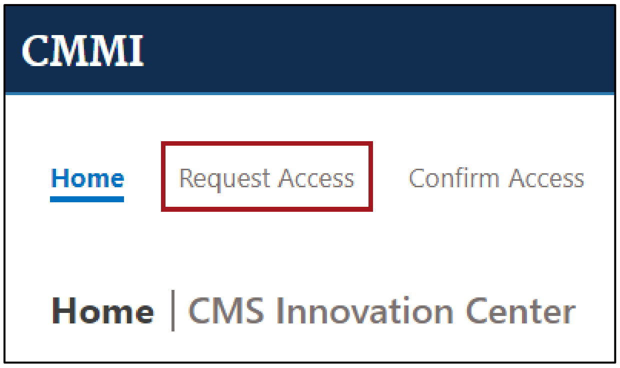
2. Click on the Innovation Center button, then click on “Application Console.”



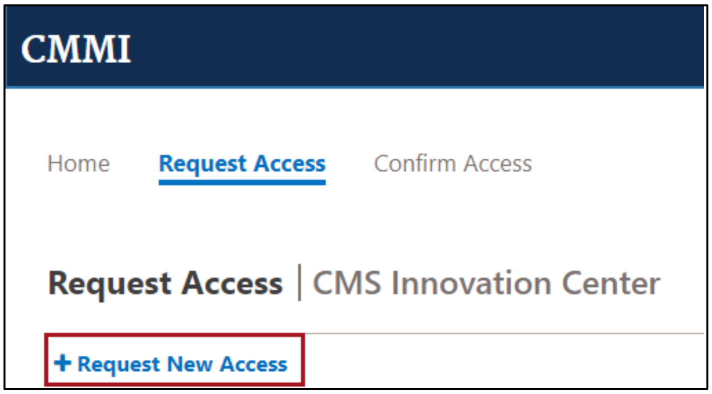
3. On the My Portal page, select the **Innovation Center** widget and then select the **Application Console** link.



4. Select **Request Access** and you will be directed to a new screen to request access.

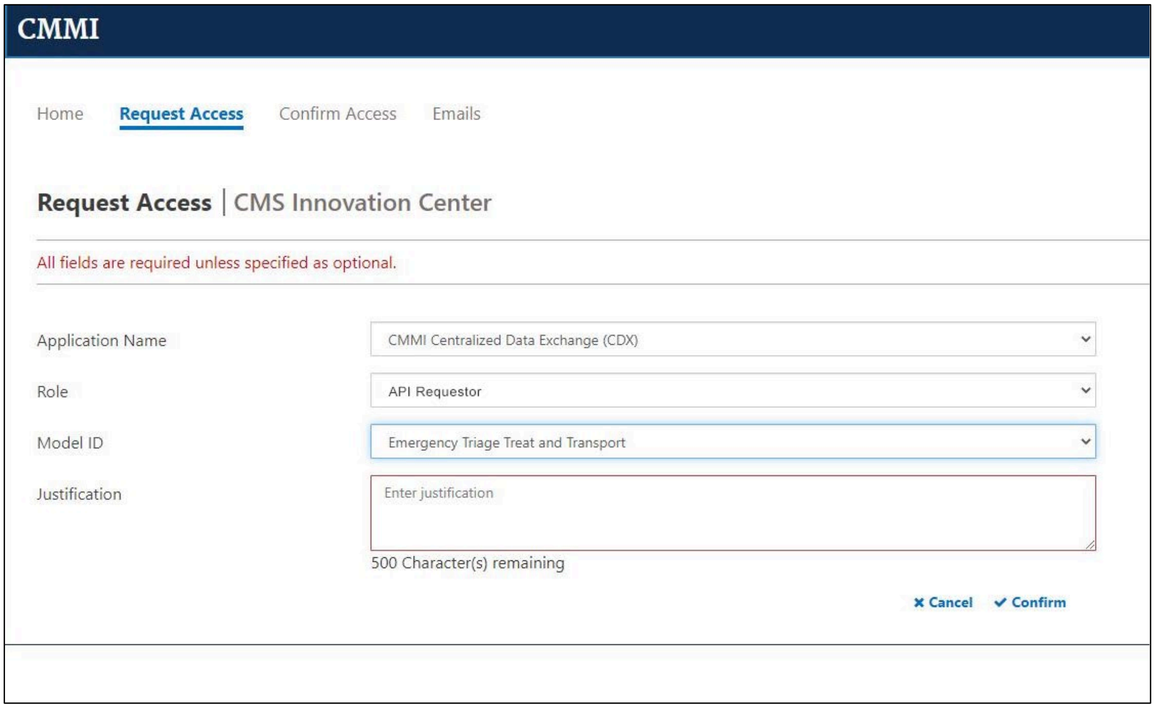


5. On the Request Access tab, select **Request New Access** and you will be directed to a new screen to make your selections.



6. On the Request Access screen, select **CMMI Centralized Data Exchange (CDX)** from the Application Name dropdown and then select your role from the Role dropdown menu.

Application permissions are granted based on user role. Depending on the role you select, the system will require additional information from you, such as Model ID and Participant ID.



All fields are required unless specified as optional.

Application Name: CMMI Centralized Data Exchange (CDX)

Role: API Requestor

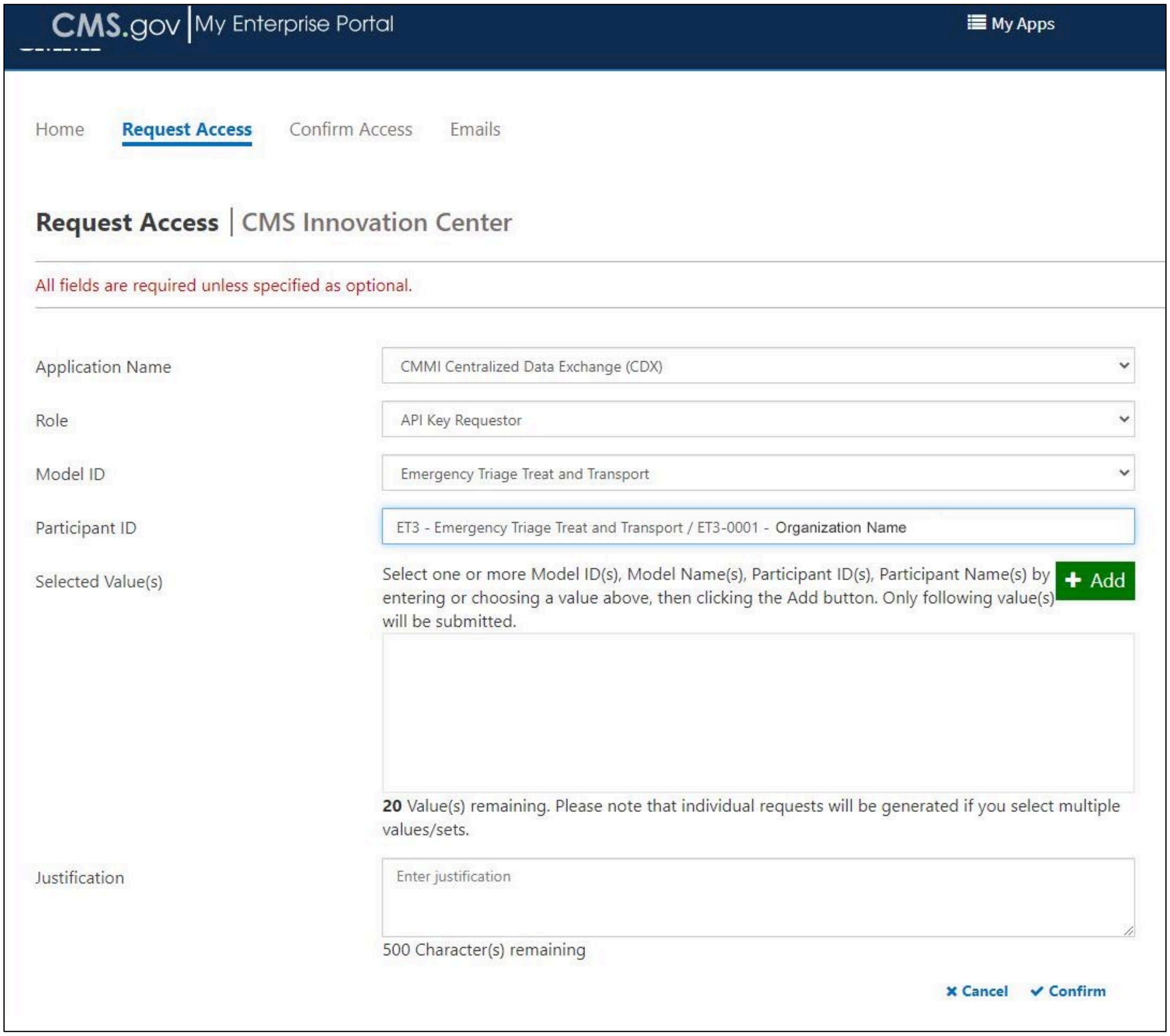
Model ID: Emergency Triage Treat and Transport

Justification: Enter justification

500 Character(s) remaining

7. If you select the Model Participant, Model Participant Representative, or API Key Requestor role, the system requires that you to select a Model ID and a Participant ID since these user roles are granted access to CMMI models at the organization level. Each organization within a model has its own Participant ID. Model teams can provide the appropriate Participant ID.

After selecting the model from the Model ID dropdown menu, begin typing the Participant ID in the Participant ID field to display Participant IDs for selection. Then select the **Add** button to add the values to your request. You can add up to 20 values/sets.

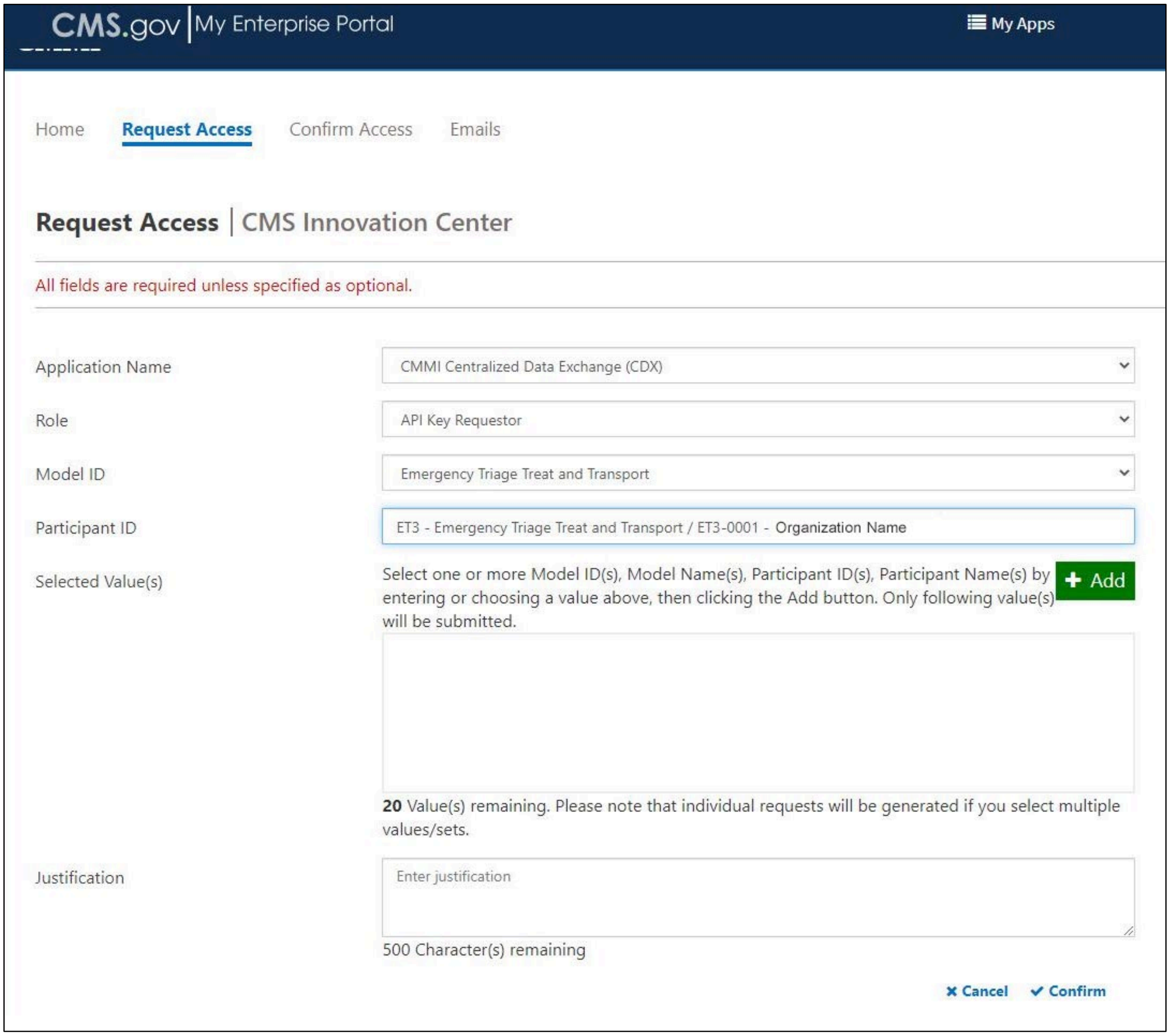


Request Access | CMS Innovation Center

All fields are required unless specified as optional.

Application Name	CMMI Centralized Data Exchange (CDX)
Role	API Key Requestor
Model ID	Emergency Triage Treat and Transport
Participant ID	ET3 - Emergency Triage Treat and Transport / ET3-0001 - Organization Name
Selected Value(s)	Select one or more Model ID(s), Model Name(s), Participant ID(s), Participant Name(s) by entering or choosing a value above, then clicking the Add button. Only following value(s) will be submitted. **20** Value(s) remaining. Please note that individual requests will be generated if you select multiple values/sets.
Justification	Enter justification 500 Character(s) remaining

8. Enter the justification for your access in the Justification field and select the **Confirm** button to submit your request. After your request is reviewed, you will receive an email notification stating whether your request was approved or denied.



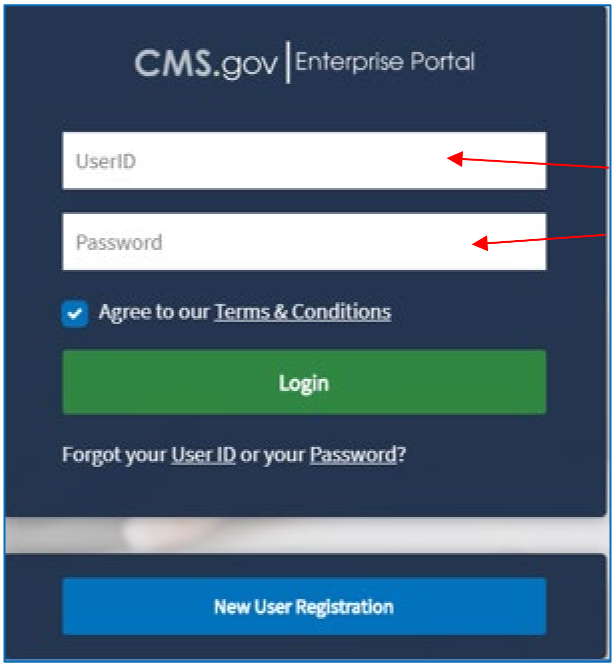
Request Access | CMS Innovation Center

All fields are required unless specified as optional.

Application Name	CMMI Centralized Data Exchange (CDX)
Role	API Key Requestor
Model ID	Emergency Triage Treat and Transport
Participant ID	ET3 - Emergency Triage Treat and Transport / ET3-0001 - Organization Name
Selected Value(s)	Select one or more Model ID(s), Model Name(s), Participant ID(s), Participant Name(s) by entering or choosing a value above, then clicking the Add button. Only following value(s) will be submitted.
	20 Value(s) remaining. Please note that individual requests will be generated if you select multiple values/sets.
Justification	Enter justification
	500 Character(s) remaining

Once your IC Application user role request is approved, you may request access to the CMMI CDX Application. To request access, complete the following steps:

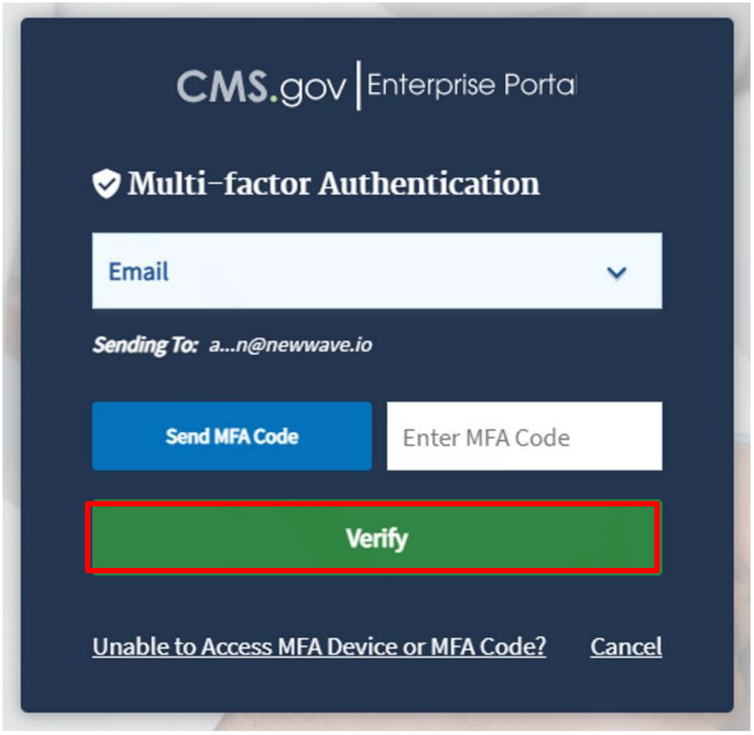
1. Go to https://portal.cms.gov/ and log in using your credentials and security code.



CMS.gov | Enterprise Portal
UserID
Password
☑ Agree to our Terms & Conditions
Login
Forgot your User ID or your Password?
New User Registration

Figure 1 - CMS ePortal Login

2. **Email** is the default option for MFA. Select the **Send MFA Code** button. Check your Email inbox for the security code and enter the numbers in the **Enter MFA Code** field then click the **Verify** button.



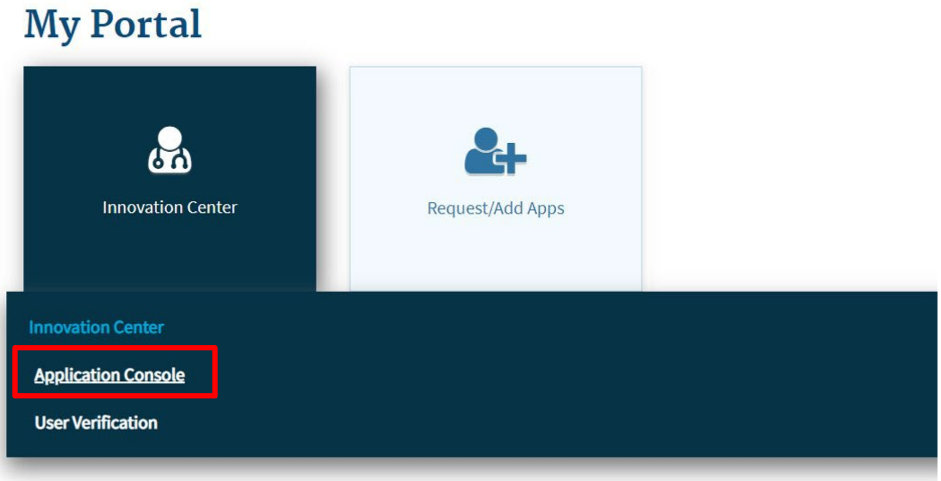
CMS.gov | Enterprise Portal

Multi-factor Authentication

Email

Sending To: a...n@newwave.io

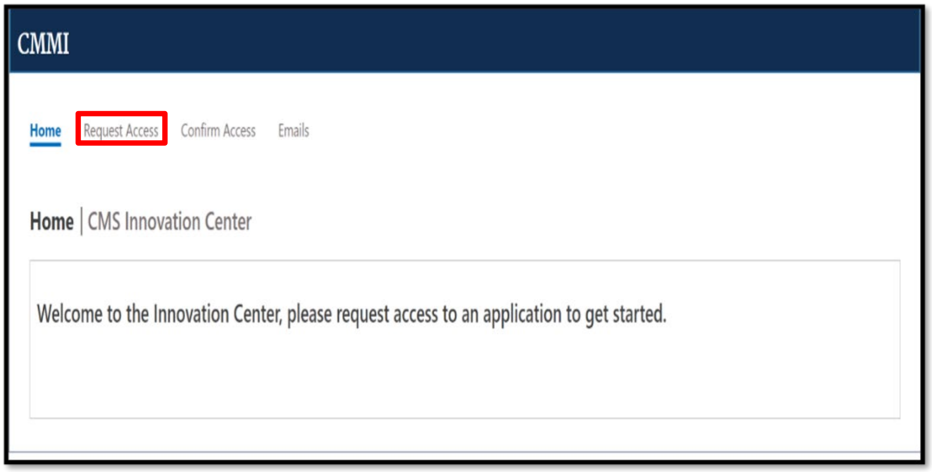
3. On the **My Portal** page, select the **Innovation Center** widget, then select the **Application Console** link.



My Portal

Figure 2 - My Portal Page

4. Select **Request Access**. You are directed to a new screen to request access.

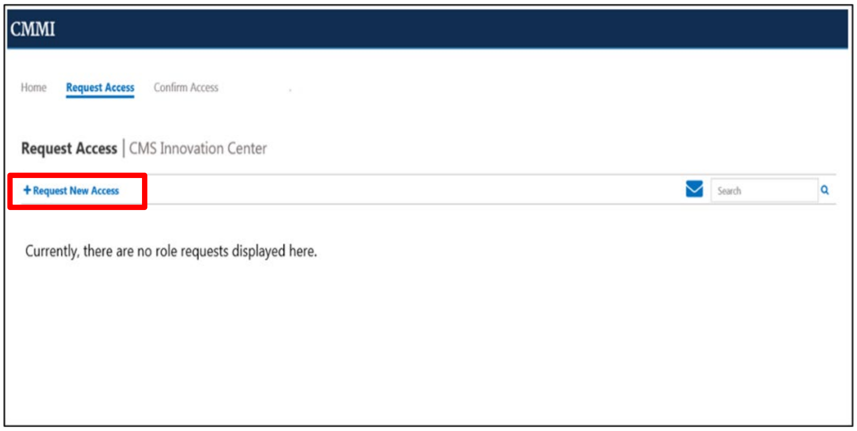


Home | CMS Innovation Center

Welcome to the Innovation Center, please request access to an application to get started.

Figure 3 - Landing Page with Request Access Highlighted

5. The IC Application Console **Home** page will not display any widgets until your access to a model has been approved.



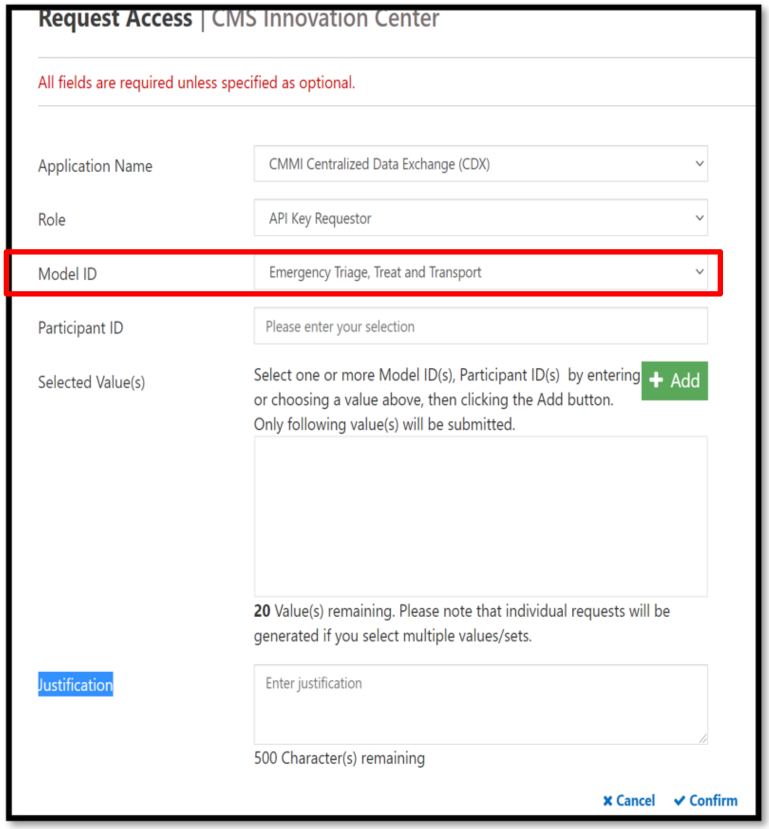
Request Access | CMS Innovation Center

Currently, there are no role requests displayed here.

Figure 4 - Request New Access Link

6. On the **Request Access** screen, select **CMMI Centralized Data Exchange (CDX)** from the **Application Name** dropdown, and select your role from the **Role** dropdown menu. Application permissions are granted based on user role. Depending on the role you select, the system requires you to provide additional information, such as Model ID and Participant ID.

7. If you select the **Model Lead** role, the system requires you to select a model from the **Model ID** dropdown menu to access that model.



Request Access | CMS Innovation Center

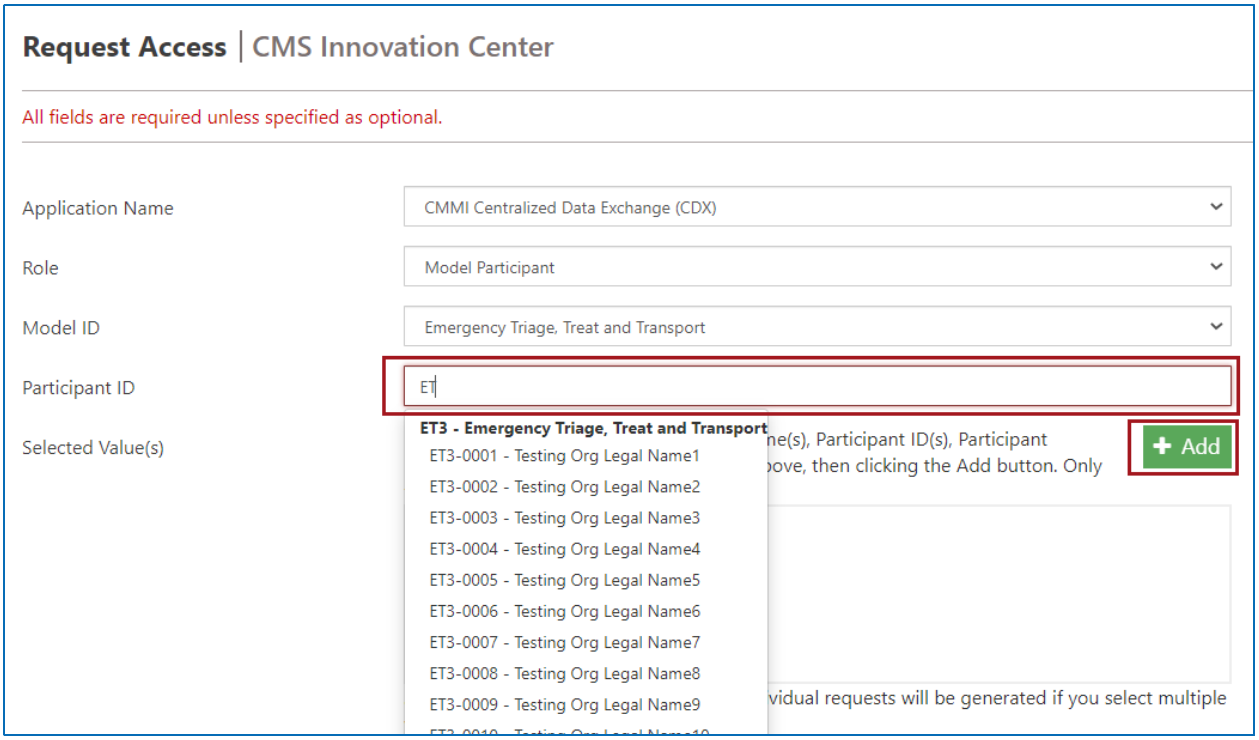
All fields are required unless specified as optional.

Application Name	CMMI Centralized Data Exchange (CDX)
Role	API Key Requestor
Model ID	Emergency Triage, Treat and Transport
Participant ID	Please enter your selection
Selected Value(s)	Select one or more Model ID(s), Participant ID(s) by entering or choosing a value above, then clicking the Add button. Only following value(s) will be submitted. **20** Value(s) remaining. Please note that individual requests will be generated if you select multiple values/sets.
Justification	Enter justification 500 Character(s) remaining

Figure 5 - Request Access Screen: Select Model ID

8. If you select the **Model Participant**, **Model Participant Representative**, or **API Key Requestor** role, the system requires you to select a Model ID and a Participant ID since these user roles have access to models at the organization level. Each organization within a model has its own Participant ID. Contact the respective Model Team for the Participant ID.

9. After selecting the model from the **Model ID** dropdown menu, begin typing the Participant ID in the **Participant ID** field to display Participant IDs for selection. Then select the **Add** button to add the values to your request. You can add up to 20 values/sets.



Request Access | CMS Innovation Center

All fields are required unless specified as optional.

Application Name	CMMI Centralized Data Exchange (CDX)
Role	Model Participant
Model ID	Emergency Triage, Treat and Transport
Participant ID	ET
Selected Value(s)	

ET3 - Emergency Triage, Treat and Transport

ET3-0001 - Testing Org Legal Name1

ET3-0002 - Testing Org Legal Name2

ET3-0003 - Testing Org Legal Name3

ET3-0004 - Testing Org Legal Name4

ET3-0005 - Testing Org Legal Name5

ET3-0006 - Testing Org Legal Name6

ET3-0007 - Testing Org Legal Name7

ET3-0008 - Testing Org Legal Name8

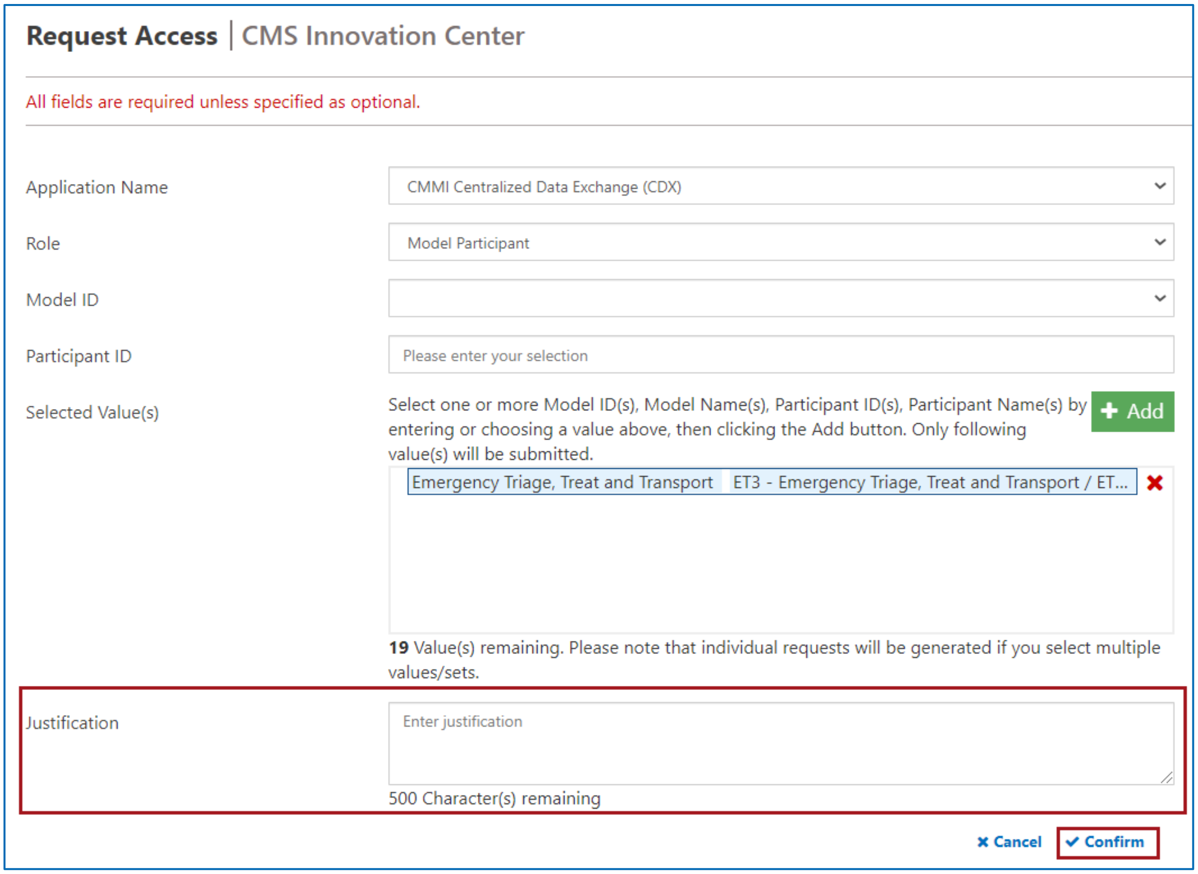
ET3-0009 - Testing Org Legal Name9

ne(s), Participant ID(s), Participant
ove, then clicking the Add button. Only

vidual requests will be generated if you select multiple

Figure 6 - Request Access Screen: Select Model ID and Participant ID

10. Enter the justification for your access in the **Justification** field and select the **Confirm** button to submit your request. After reviewing your request, you will receive an email notification stating whether the Model Team approved or denied your request.



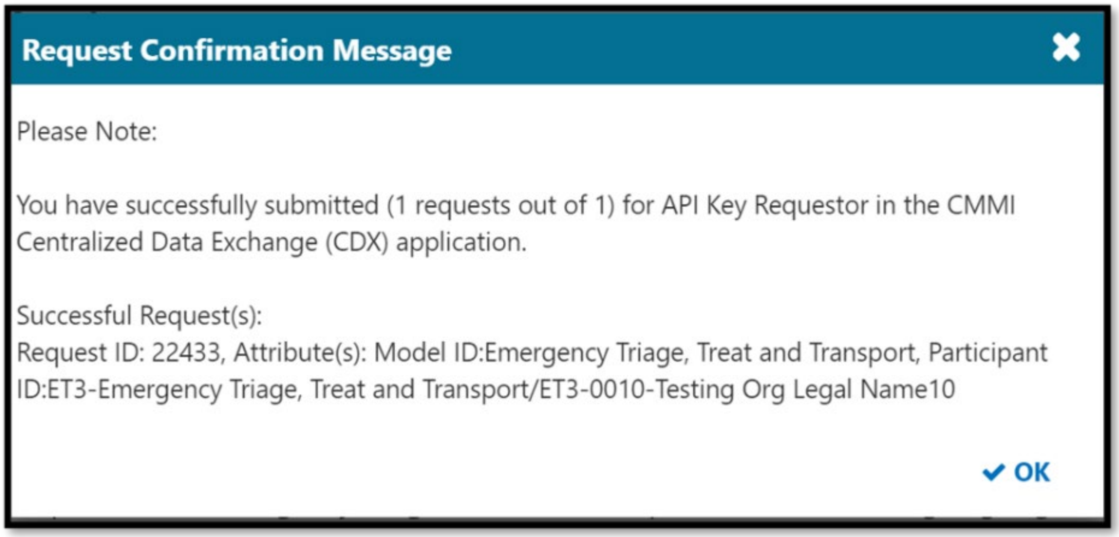
Request Access | CMS Innovation Center

All fields are required unless specified as optional.

Application Name	CMMI Centralized Data Exchange (CDX)
Role	Model Participant
Model ID	
Participant ID	Please enter your selection
Selected Value(s)	Select one or more Model ID(s), Model Name(s), Participant ID(s), Participant Name(s) by entering or choosing a value above, then clicking the Add button. Only following value(s) will be submitted. Emergency Triage, Treat and Transport ET3 - Emergency Triage, Treat and Transport / ET... **19** Value(s) remaining. Please note that individual requests will be generated if you select multiple values/sets.
Justification	Enter justification 500 Character(s) remaining

Figure 7 - Request Access Screen: Enter Justification and Select Confirm

11. Users will receive an onscreen and email confirmation for each Role Request that they submit. Select the **OK** button to close the Request Confirmation window.



Request Confirmation Message

Please Note:

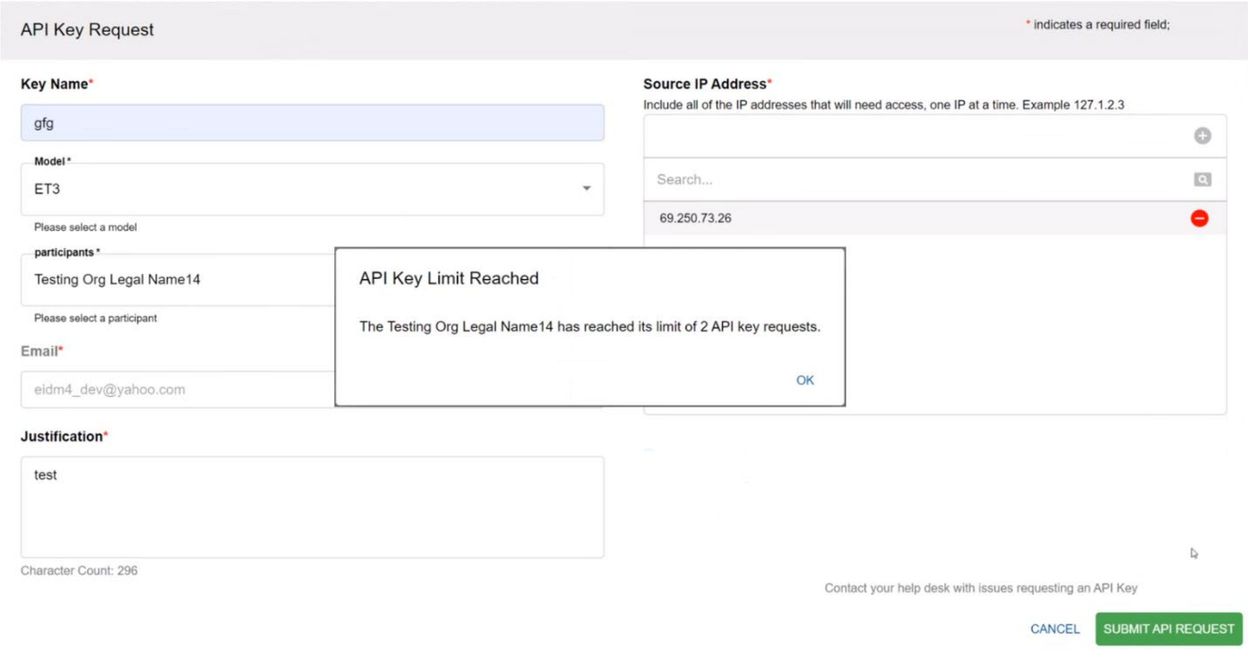
You have successfully submitted (1 requests out of 1) for API Key Requestor in the CMMI Centralized Data Exchange (CDX) application.

Successful Request(s):
Request ID: 22433, Attribute(s): Model ID:Emergency Triage, Treat and Transport, Participant ID:ET3-Emergency Triage, Treat and Transport/ET3-0010-Testing Org Legal Name10

Figure 8 - Request Access Screen: Enter Justification and Select Confirm

After acquiring a User ID and Password, you will then request an ET3 Security Authentication Key, which will be used on each data transmission to and from CMS (see Appendix A, Flow 2a).

Note: You must have the CDX API Key Requestor role to complete this task.
You can submit two API Key requests per organization. If you have already requested two keys for an organization, deactivate an existing key request, and submit a new request. The application displays a notification when you have reached the maximum number of requests.



API Key Request

* indicates a required field;

Key Name*: gfg

Model*: ET3

Please select a model

participants*: Testing Org Legal Name14

Please select a participant

Email*: eidm4_dev@yahoo.com

Justification*: test

Character Count: 296

Source IP Address*

Include all of the IP addresses that will need access, one IP at a time. Example 127.1.2.3

Search...

69.250.73.26

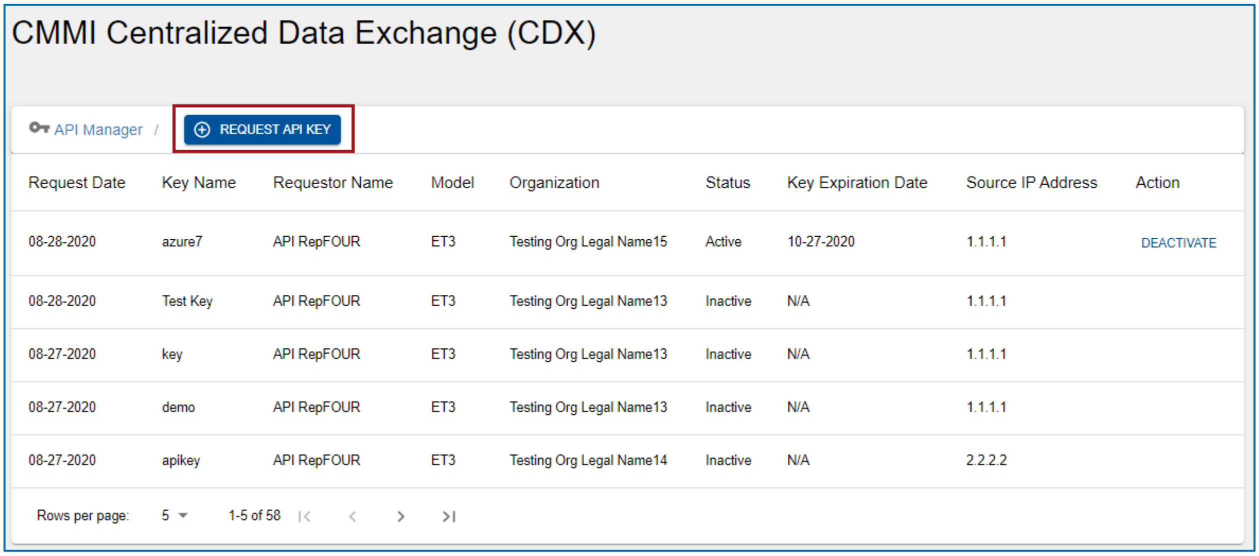
API Key Limit Reached

The Testing Org Legal Name14 has reached its limit of 2 API key requests.

Contact your help desk with issues requesting an API Key

Figure 9 - API Key Limit Exceeded Error

1. On the **API Manager** page, select the **REQUEST API KEY** button.



CMMI Centralized Data Exchange (CDX)

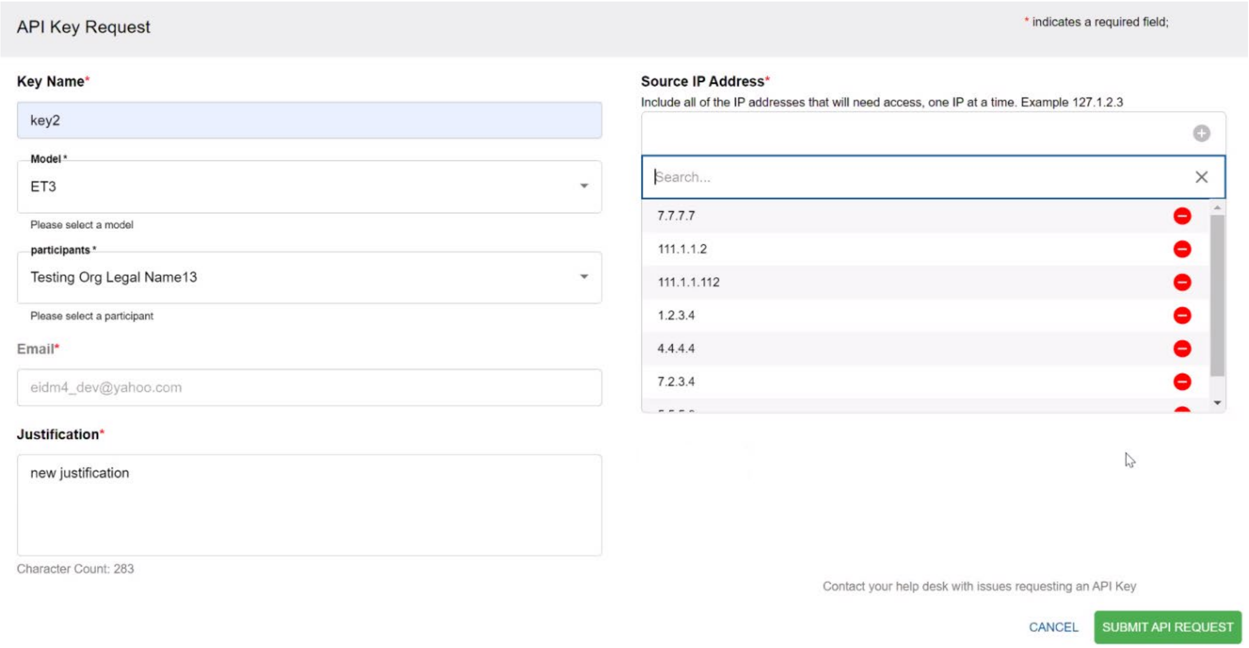
Request Date	Key Name	Requestor Name	Model	Organization	Status	Key Expiration Date	Source IP Address	Action
08-28-2020	azure7	API RepFOUR	ET3	Testing Org Legal Name15	Active	10-27-2020	1.1.1.1	DEACTIVATE
08-28-2020	Test Key	API RepFOUR	ET3	Testing Org Legal Name13	Inactive	N/A	1.1.1.1	
08-27-2020	key	API RepFOUR	ET3	Testing Org Legal Name13	Inactive	N/A	1.1.1.1	
08-27-2020	demo	API RepFOUR	ET3	Testing Org Legal Name13	Inactive	N/A	1.1.1.1	
08-27-2020	apikey	API RepFOUR	ET3	Testing Org Legal Name14	Inactive	N/A	2.2.2.2	

Rows per page: 5 1-5 of 58

Figure 10 - Request API Key Button

2. The API Key Request form is displayed. Provide the **Key Name**, **Model**, **Organization**, **Source IP**, **Email**, and **Justification** details. Select **SUBMIT API REQUEST**.
3. It is important to note that the user must use valid IP addresses for the Source IP field. The system validates Source IP Address format. If the IP address format is not valid, the user will not be able to add an invalid IP Address.

Note: The IP Address must be the IP Address that the user is sending the PCRs from, it should not be a private internal IP address or the user home IP address.



API Key Request

* indicates a required field;

Key Name*: key2

Model *: ET3

Please select a model

participants *: Testing Org Legal Name13

Please select a participant

Email*: eidm4_dev@yahoo.com

Justification*: new justification

Character Count: 283

Source IP Address*

Include all of the IP addresses that will need access, one IP at a time. Example 127.1.2.3

Search...

7.7.7.7

111.1.1.2

111.1.1.112

1.2.3.4

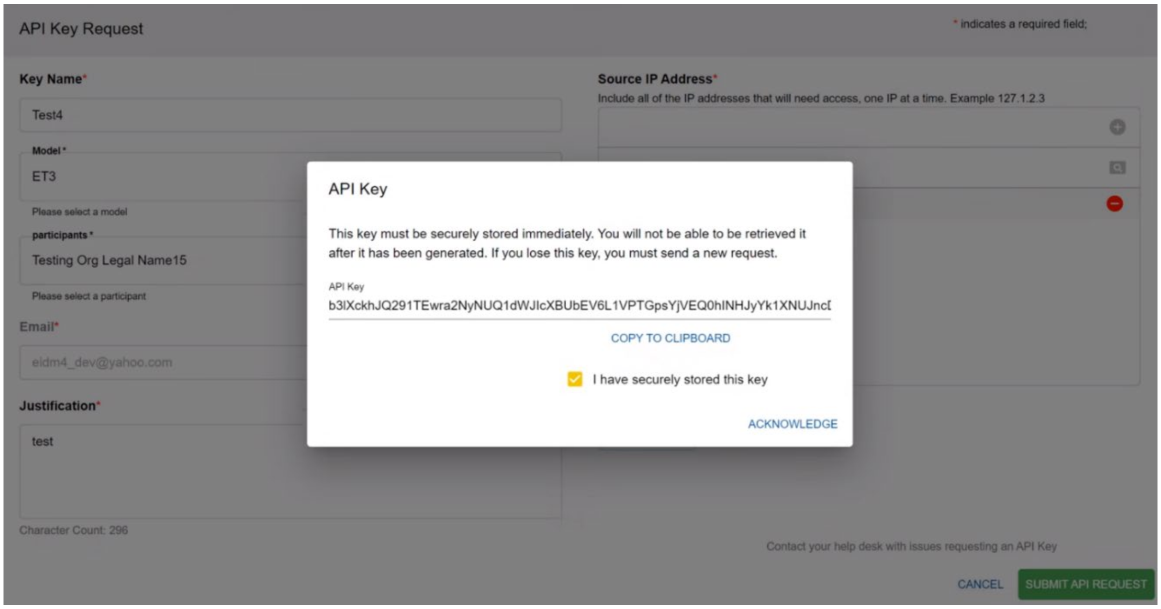
4.4.4.4

7.2.3.4

Contact your help desk with issues requesting an API Key

Figure 11 - API Key Request Form

4. The **API Key** pop-up window displays. To save the key, select **COPY TO CLIPBOARD** and then immediately store the key in a secure place. You will need to submit a new request if you lose the key. Once you have stored the key, select the **I have securely stored this key** checkbox and then select **ACKNOWLEDGE**.



API Key Request

* indicates a required field;

Key Name*
Test4

Model *
ET3
Please select a model

participants *
Testing Org Legal Name15
Please select a participant

Email*
eldm4_dev@yahoo.com

Justification*
test
Character Count: 296

Source IP Address*
Include all of the IP addresses that will need access, one IP at a time. Example 127.1.2.3

API Key

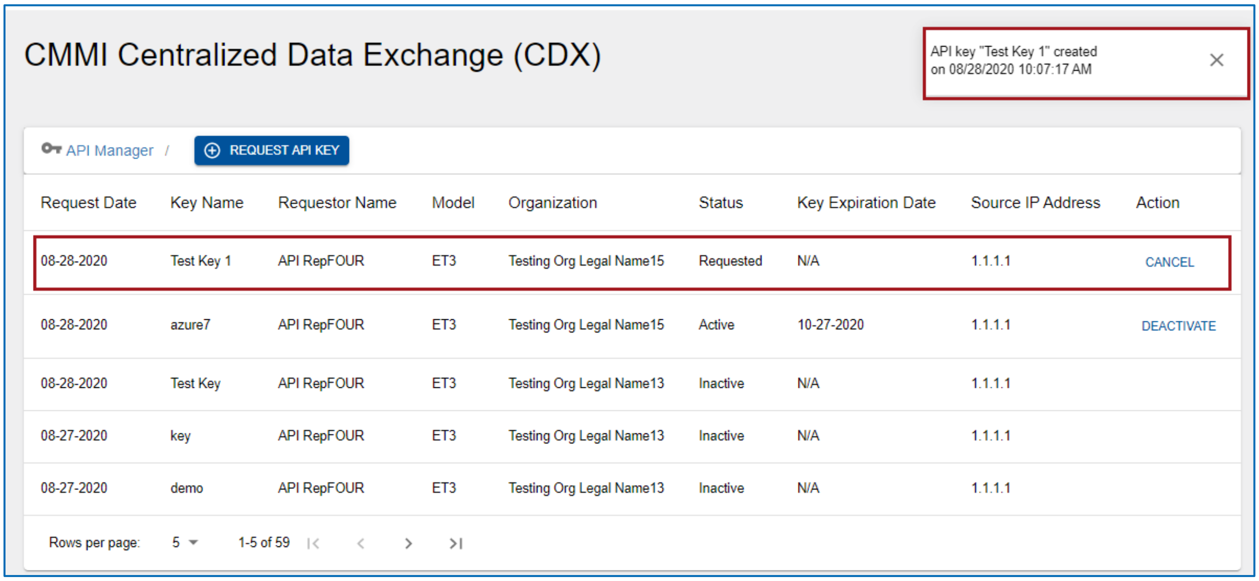
This key must be securely stored immediately. You will not be able to be retrieved it after it has been generated. If you lose this key, you must send a new request.

API Key
b3IXckhJQ291TEwra2NyNUQ1dWJlcXBUbEV6L1VPTGpsYjVEQ0hINHJyYk1XNUJncI

COPY TO CLIPBOARD
☑ I have securely stored this key
ACKNOWLEDGE
Contact your help desk with issues requesting an API Key
CANCEL
SUBMIT API REQUEST

Figure 12 - API Key Window

5. The application displays a notification that the API Key has been created. The request displays with a status of “Requested” in the **API Key Management** table. The Model Lead then needs to review your request. The key is ready for use when the Model Lead approves the request, and the status displays as “Active” in the **Status** column.



CMMI Centralized Data Exchange (CDX)

API key "Test Key 1" created on 08/28/2020 10:07:17 AM

Request Date	Key Name	Requestor Name	Model	Organization	Status	Key Expiration Date	Source IP Address	Action
08-28-2020	Test Key 1	API RepFOUR	ET3	Testing Org Legal Name15	Requested	N/A	1.1.1.1	CANCEL
08-28-2020	azure7	API RepFOUR	ET3	Testing Org Legal Name15	Active	10-27-2020	1.1.1.1	DEACTIVATE
08-28-2020	Test Key	API RepFOUR	ET3	Testing Org Legal Name13	Inactive	N/A	1.1.1.1	
08-27-2020	key	API RepFOUR	ET3	Testing Org Legal Name13	Inactive	N/A	1.1.1.1	
08-27-2020	demo	API RepFOUR	ET3	Testing Org Legal Name13	Inactive	N/A	1.1.1.1	

Rows per page: 5 ▾ 1-5 of 59

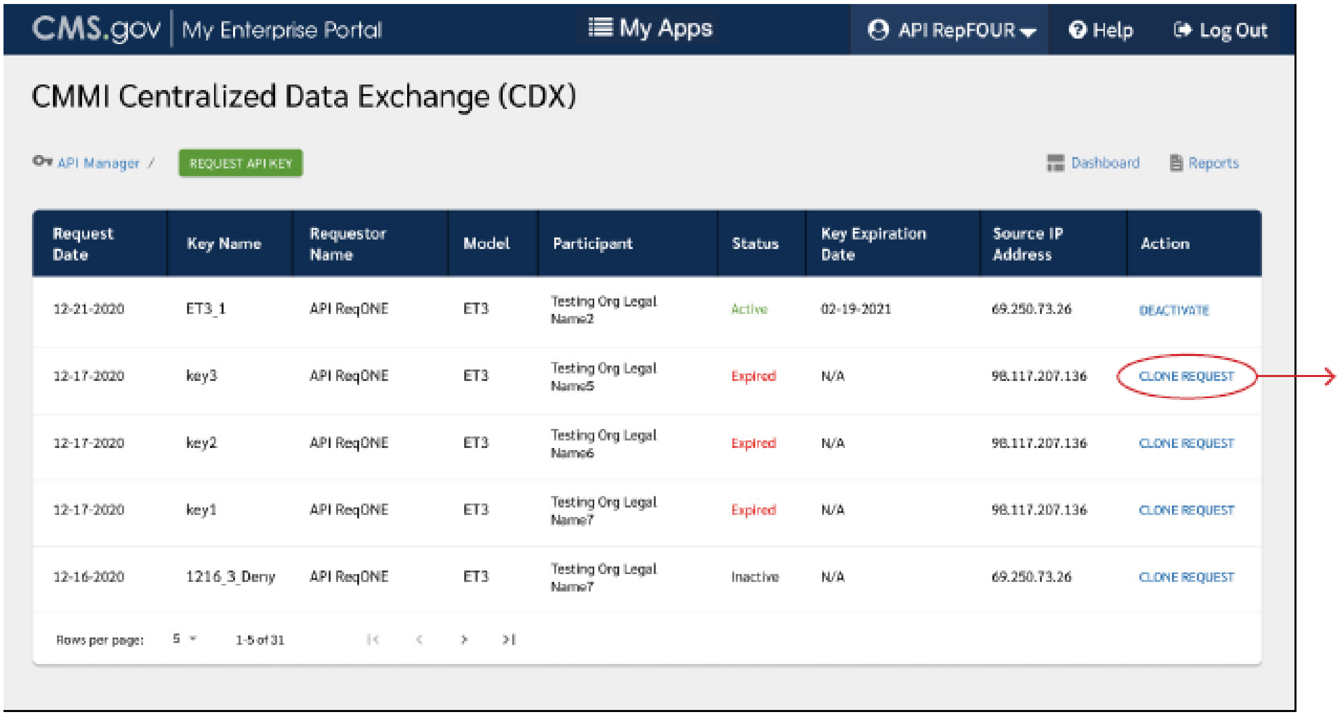
Figure 13 - Notification Confirming Request and New Request Displayed with Requested Status

After acquiring an ET3 Security Authentication Key, you will be required to renew the API Key every 180 days.

NOTE: IF AN API KEY IS EXPIRED OR INACTIVE THE "CLONE REQUEST" LINK WILL APPEAR IN THE ACTIONS COLUMN.

Here are a few required steps to use the "Clone Request" functionality:

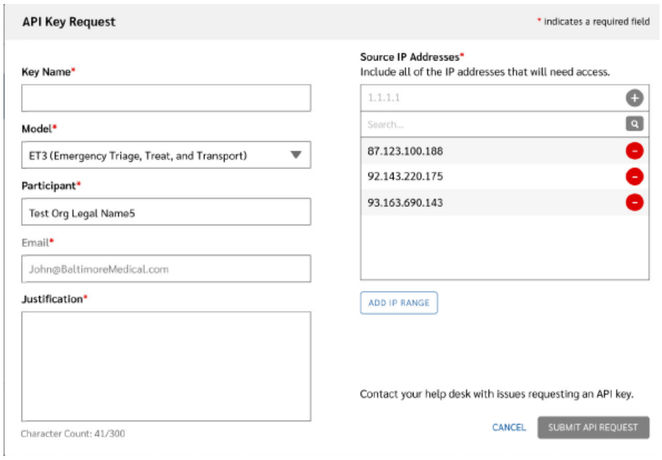
- THE FORM WILL PREPOPULATE WITH THE PREVIOUSLY SUBMITTED INFORMATION.
- THE USER WILL NEED TO ENTER A NEW KEY NAME AND JUSTIFICATION.
- THE USER CAN ALSO ADD AND REMOVE IP ADDRESSES.



CMMI Centralized Data Exchange (CDX)

Request Date	Key Name	Requestor Name	Model	Participant	Status	Key Expiration Date	Source IP Address	Action
12-21-2020	ET3_1	API ReqONE	ET3	Testing Org Legal Name2	Active	02-19-2021	69.250.73.26	DEACTIVATE
12-17-2020	key3	API ReqONE	ET3	Testing Org Legal Name5	Expired	N/A	98.117.207.136	CLONE REQUEST
12-17-2020	key2	API ReqONE	ET3	Testing Org Legal Name6	Expired	N/A	98.117.207.136	CLONE REQUEST
12-17-2020	key1	API ReqONE	ET3	Testing Org Legal Name7	Expired	N/A	98.117.207.136	CLONE REQUEST
12-16-2020	1216_3_Deny	API ReqONE	ET3	Testing Org Legal Name7	Inactive	N/A	69.250.73.26	CLONE REQUEST

Rows per page: 5 1-5 of 31



API Key Request

* indicates a required field

Key Name*

Model*
ET3 (Emergency Triage, Treat, and Transport)

Participant*
Test Org Legal Name5

Email*
John@BaltimoreMedical.com

Justification*

Character Count: 41/300

Source IP Addresses*
Include all of the IP addresses that will need access.

1.1.1.1

Search...

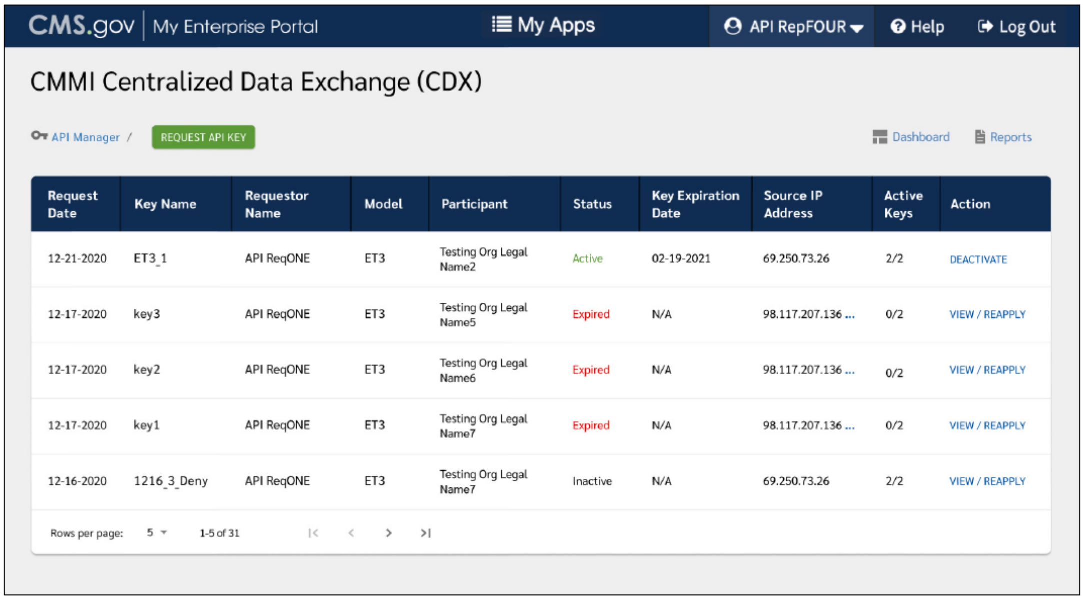
87.123.100.188

92.143.220.175

93.163.690.143

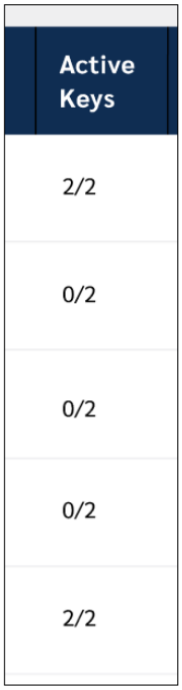
Contact your help desk with issues requesting an API key.

After renewing your ET3 Security Authentication Key, you can track the number of ACTIVE keys associated with each API Key request made using the API Key Manager page:



CMMI Centralized Data Exchange (CDX)

Request Date	Key Name	Requestor Name	Model	Participant	Status	Key Expiration Date	Source IP Address	Active Keys	Action
12-21-2020	ET3_1	API ReqONE	ET3	Testing Org Legal Name2	Active	02-19-2021	69.250.73.26	2/2	DEACTIVATE
12-17-2020	key3	API ReqONE	ET3	Testing Org Legal Name5	Expired	N/A	98.117.207.136 ...	0/2	VIEW / REAPPLY
12-17-2020	key2	API ReqONE	ET3	Testing Org Legal Name6	Expired	N/A	98.117.207.136 ...	0/2	VIEW / REAPPLY
12-17-2020	key1	API ReqONE	ET3	Testing Org Legal Name7	Expired	N/A	98.117.207.136 ...	0/2	VIEW / REAPPLY
12-16-2020	1216_3_Deny	API ReqONE	ET3	Testing Org Legal Name7	Inactive	N/A	69.250.73.26	2/2	VIEW / REAPPLY



Active Keys
2/2
0/2
0/2
0/2
2/2