



Centers for Medicare & Medicaid Services

Enterprise Privacy Policy Engine Cloud (EPPE)

Training Module - User Registration Process

Version 2.1

06/03/2026

Document Number: EPPE-299-IDM-v2.1

Table of Contents

1	Overview	1
1.1	EPPE Access Prerequisites	1
1.2	Icons Used Throughout the EPPE System	1
2	About EPPE	2
2.1	Identify Management (IDM) Introduction	2
2.2	Multi-Factor Authentication (MFA) Overview	2
2.3	IDM Registration Process	3
2.4	EPPE Registration Process	8
2.5	Experian Identity Verification	11
2.6	Requesting Access to EPPE.....	13
2.7	Requesting Access to EPPE Roles.....	15
3	Acronyms and Glossary.....	18
4	EPPE Help Desk Information	19

List of Figures

Figure 1:	IDM Registration URL Address	3
Figure 2:	IDM Registration Login Page	3
Figure 3:	IDM Sign In/Create your CMS Account Page.....	4
Figure 4:	IDM Login/Create your CMS Account Page	4
Figure 5:	IDM User Registration Page Personal Section Part 1	5
Figure 6:	IDM User Registration Page Personal Section Part 2	5
Figure 7:	IDM User Registration Page Contact Section	6
Figure 8:	IDM User Registration Page Credentials Section User ID.....	6
Figure 9:	IDM User Registration Page Credentials Section Password	7
Figure 10:	IDM User Registration Page Credentials Section Security Question and Answer	7
Figure 11:	IDM Registration Confirmation	8
Figure 12:	IDM Login Page	8
Figure 13:	IDM Sign In/Create your CMS Account Page.....	9
Figure 14:	IDM Sign In/Create your CMS Account Page User ID and Password.....	9
Figure 15:	IDM Multi-Factor Authentication Request.....	10
Figure 16:	IDM Multi-Factor Authentication Request Enter Code.....	10

Figure 17: IDM My Portal Page	10
Figure 18: Requesting Access Role Selection	11
Figure 19: Requesting Access Identity Verification	11
Figure 20: Identity Verification Step 1.....	12
Figure 21: Identity Verification Step 2.....	12
Figure 22: Identity Verification Step 3.....	13
Figure 23: Identity Verification Confirmation.....	13
Figure 24: Requesting Access Role Details	14
Figure 25: Requesting Access Reason for Request.....	14
Figure 26: Requesting Access Confirmation Request.....	15
Figure 27: Requesting Access Confirmation Message.....	15
Figure 28: Requesting Access My Access Page.....	15
Figure 29: Requesting an EPPE Role My Portal Page.....	15
Figure 30: Requesting an EPPE Role EPPE First Time User Page.....	16
Figure 31: Requesting an EPPE Role Request a Role in EPPE Pop-Out Window	16
Figure 32: EPPE Role Request Attestation.	17
Figure 33: Requesting an EPPE Role Confirmation.....	17

List of Tables

Table 1: Acronyms	18
-------------------------	----

1 Overview

This Training Guide will cover the following:

- EPPE Overview
- IDM Overview
- Multi-Factor Authentication (MFA) Overview
- IDM Registration Process
- EPPE Registration Process
- Experian Identity Verification
- Requesting Access to EPPE
- Requesting Access to EPPE Roles

1.1 EPPE Access Prerequisites

Before continuing this training, please complete the following:

- Obtain Identity Management (IDM) Credentials, Multi-Factor Authentication (MFA), and EPPE Access: <https://www.cms.gov/files/document/eppeidm.pdf>
- Access CMS Portal: <https://portal.cms.gov/>

1.2 Icons Used Throughout the EPPE System



A red asterisk denotes that a field is required to be entered.



The question mark icon, when selected, will display field specific help.

2 About EPPE

The Enterprise Privacy Policy Engine (EPPE) system automates the process of submitting Data Use Agreement (DUA) requests and tracking their status through the approval and data receipt stages. End users, (requesters and all CMS approvers), can interactively use the system to manage their DUAs. For those requests that require supporting documentation, it allows documents to be uploaded and then later downloaded for review.

The EPPE Application processes the following 4 DUA Customer Types:

- Contractor
- Limited Data Sets
- Researcher
- Non-DUA Tracking Requests

This training will guide you through the steps necessary to gain access to the EPPE system.

2.1 Identify Management (IDM) Introduction

The IDM system used by EPPE provides users with access to CMS applications. The CMS established IDM to provide business partners with a means to create a single User ID that they can use to access one or more CMS applications.

To apply and receive an IDM User ID, complete the steps that follow.

2.2 Multi-Factor Authentication (MFA) Overview

Multi-Factor Authentication (MFA) is generally required to access CMS sensitive data. The MFA uses a combination of two (or more) different token attributes (also known as factors), to authenticate the user. The EPPE Application requires two types of authentications.

- The first factor is what users know. This is usually a password, but this can also include a user response to a secret challenge question. This is generally known as Knowledge Based Authentication, and by itself, is insufficient for authentication to most CMS sensitive information.
- The second factor is what users have. This could be a physical object (hard token), for example, a smart card, or hardware token that generates one-time-only passwords. It might also be some encrypted software token (soft token) installed on an individual's system (usually with very limited functional parameters for use).

Note: Some MFA options require the installation of an application on a smartphone.

The available MFA Options are listed below:

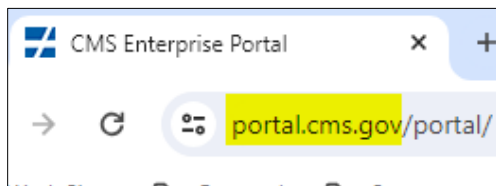
- **Email** – This is the default option that is initially used to access IDM for the first time. Once the user logs in successfully, the user can specify any or all of the other MFA options through a profile update or continue to use email. Email is the only option that cannot be removed and will always remain on your profile.
- **Short Message Service (SMS)** – The SMS option will send your MFA Code directly to your mobile device via a text message. This option requires you to provide a ten-digit U.S. phone number for a mobile device that is capable of receiving text messages. A carrier service charge may apply for this option.

- **Interactive Voice Response (IVR)** – The IVR option will communicate your MFA Code through a voice message that will be sent directly to your phone. This option requires you to provide a valid 10-digit U.S. phone number and (optional) extension that will be used during login to obtain the MFA Code.
- **Google Authenticator** – The Google Authenticator is an application for your smart phone that generates security codes. You will be asked for a security code whenever you need to verify your identity. Supported phones include iPhone, Android Phone, and Blackberry (a download to user's smartphone is required).
- **Okta Verify** – The Okta Verify option produces push notifications which enable you to verify your identity with a single tap on your mobile device, without the need to type a code. Supported phones include iPhone, Android Phone, and Windows Phone (a download to user's smartphone is required).

2.3 IDM Registration Process

This step will guide you through creating your IDM profile, which will require both your personal and business-related information.

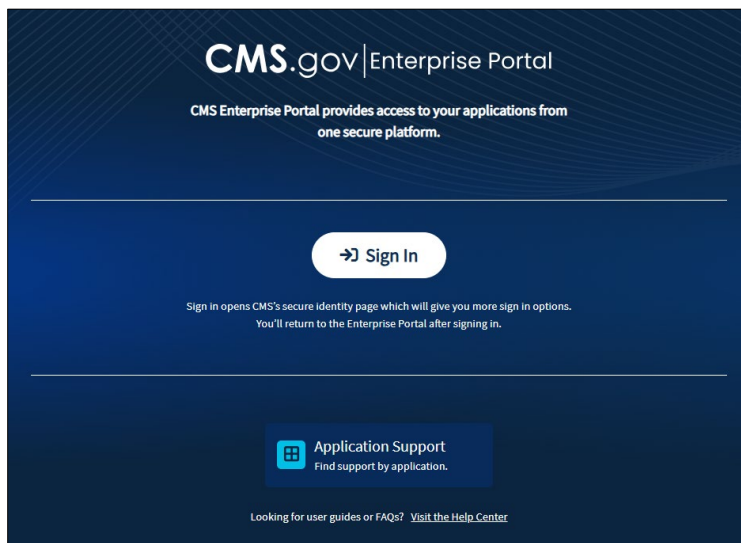
Figure 1: IDM Registration URL Address



1. Navigate to <https://portal.cms.gov>

The CMS Enterprise Portal is displayed.

Figure 2: IDM Registration Login Page



1. Click **Sign In**.

The IDM Sign In/Create a CMS account page displayed.

Figure 3: IDM Sign In/Create your CMS Account Page

The screenshot shows the 'Sign in/Create your CMS account' page. At the top, it says 'By signing in, you agree to the [terms and conditions](#).' Below this are four sign-in options, each with a 'Continue' button:

- Personal Identity Verification (PIV)**: Existing CMS employees and contractors can securely sign in using their federal PIV card.
- ID.me**: Trusted and used by federal services like Medicare.gov and Social Security.
- Login.gov**: New users should choose this trusted sign-in option to create an account or sign in with existing Login.gov credentials.
- EUA or IDM User ID**: Existing users with active EUA or IDM credentials can sign in using their current account.

At the bottom, there is an 'FAQs' section with two links: 'How do I know which [sign in option](#) to choose?' and 'Why does this [sign in page](#) look different?'

1. Click **Continue** on the EUA or IDM User ID option.

The IDM Login/Create a CMS account page displayed.

Figure 4: IDM Login/Create your CMS Account Page

The screenshot shows the 'Login/Create your CMS account' page. It has two input fields: 'User ID' and 'Password'. The 'User ID' field has a red error message: 'This field cannot be left blank'. Below the input fields is a large blue 'Sign in' button. At the bottom, there is a section titled 'Having issues signing in?' with the text 'Manage your IDM/EUA credentials at the links below.' and several links: 'Forgot IDM User ID', 'EUA Login Form', 'Forgot IDM Password', 'Forgot EUA Password', 'IDM User Registration' (highlighted in yellow), 'Unlock IDM Account', and 'Help Center'. At the very bottom, there is a link: '< Back to main sign-in page'.

1. Click **IDM User Registration**.

The IDM User Registration Page is displayed on the Personal section.

Figure 5: IDM User Registration Page Personal Section Part 1

IDM User Registration

Already have a Login.gov account?
Save time by registering with your Login.gov account. If you have signed in to CMS IDM before, you may not register a new account.

1 Sign in with **LOGIN.GOV**

1 Personal **2** Contact **3** Credentials

Personal information
Enter your personal information to begin the IDM user registration process.

*Required Field

First Name*
The First Name field is required.

Middle Name

Last Name*

Suffix

Date Of Birth*
MM/DD/YYYY

E-mail Address*

Confirm E-mail Address*

1. Complete all required information.

Figure 6: IDM User Registration Page Personal Section Part 2

E-mail Address*

Confirm E-mail Address*

View Terms & Conditions

☐ I agree to the terms and conditions

Cancel **Next**

1. Click **View Terms & Conditions**
2. Click **I agree to the terms and Conditions** checkbox.
3. Click **Next**.

Note: Please provide your business email address. All other information provided should be your personal information.

The IDM User Registration Page is displayed on the Contact section.

Figure 7: IDM User Registration Page Contact Section

1. Complete all required fields

The IDM User Registration Page is displayed on the Credentials section.

Figure 8: IDM User Registration Page Credentials Section User ID

1. Enter **User ID**.

Figure 9: IDM User Registration Page Credentials Section Password

IDM User Registration

Personal Contact Credentials

Create Your Credentials

User IDs must be 6 to 74 alphanumeric characters, cannot contain more than 8 consecutive numbers, cannot begin or end with a special character, and cannot contain more than one consecutive special character. The @ symbol is only allowed if the User ID is in a valid email address format.

Passwords must:

- Be at least 15 characters long
- Contain at least one uppercase letter
- Contain at least one lowercase letter
- Contain at least one number

Special characters are optional. The following special characters are acceptable: ! # \$ % & ' () * + , - . / \ : ; < = > ? @ [] ^ _ { | } ~. Passwords cannot contain parts of the User ID, first or last name, and must be different than the last six password used. Users can only change their own password once every 24 hours. If a user requires a second password change within the same 24-hour period, they must contact their application help desk for assistance.

***Required Field**

User ID*

The User ID field is required.

New Password*

Confirm Password*

Security Questions*

Answer*

Cancel Back Submit

1. Enter **Password**.
2. Re-enter and **Confirm Password**.

Figure 10: IDM User Registration Page Credentials Section Security Question and Answer

IDM User Registration

Personal Contact Credentials

Create Your Credentials

User IDs must be 6 to 74 alphanumeric characters, cannot contain more than 8 consecutive numbers, cannot begin or end with a special character, and cannot contain more than one consecutive special character. The @ symbol is only allowed if the User ID is in a valid email address format.

Passwords must:

- Be at least 15 characters long
- Contain at least one uppercase letter
- Contain at least one lowercase letter
- Contain at least one number

Special characters are optional. The following special characters are acceptable: ! # \$ % & ' () * + , - . / \ : ; < = > ? @ [] ^ _ { | } ~. Passwords cannot contain parts of the User ID, first or last name, and must be different than the last six password used. Users can only change their own password once every 24 hours. If a user requires a second password change within the same 24-hour period, they must contact their application help desk for assistance.

***Required Field**

User ID*

The User ID field is required.

New Password*

Confirm Password*

Security Questions*

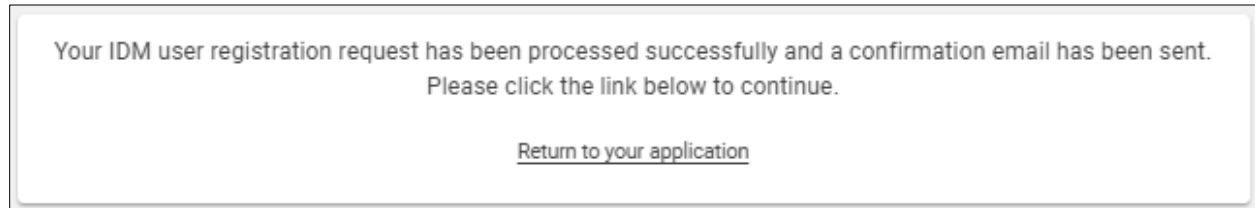
Answer*

Cancel Back Submit

1. Select **Security Question** from the dropdown menu.
2. Enter **Security Answer**.
3. Select **Submit**.

A User Registration confirmation message is displayed.

Figure 11: IDM Registration Confirmation



1. The Confirmation Message states, ***“Your IDM user registration request has been processed successfully and a confirmation email has been sent. Please click the link below to continue.”***

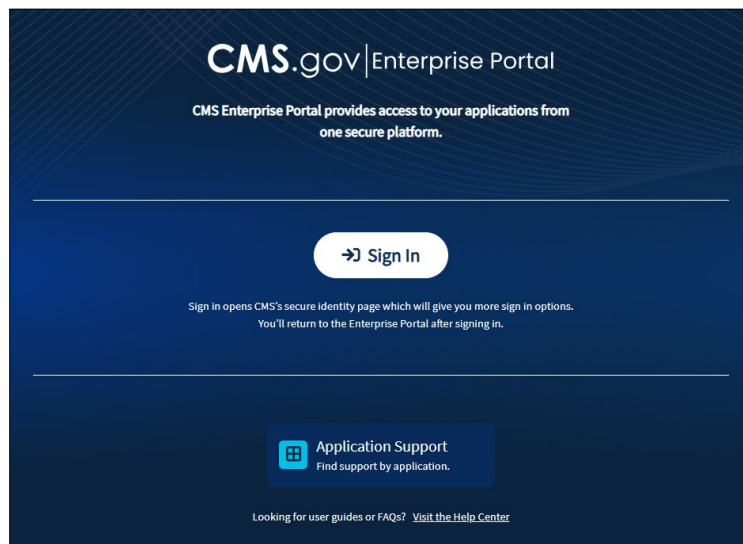
The IDM Registration Process is now complete. You will receive an email notifying you of the successful creation of your account.

2.4 EPPE Registration Process

EPPE is accessible through the CMS Enterprise Portal by using a valid Identity Management (IDM) User ID.

Note: Users must use an IDM User ID, not an Enterprise User Administration (EUA) User ID, to access the EPPE application.

Figure 12: IDM Login Page



1. Click **Sign In**.

Figure 13: IDM Sign In/Create your CMS Account Page

Sign in/Create your CMS account

By signing in, you agree to the [terms and conditions](#).

Personal Identity Verification (PIV)
Existing CMS employees and contractors can securely sign in using their federal PIV card. [Continue](#)

ID.me
Trusted and used by federal services like Medicare.gov and Social Security. [Continue](#)

Login.gov
New users should choose this trusted sign-in option to create an account or sign in with existing Login.gov credentials. [Continue](#)

EUA or IDM User ID
Existing users with active EUA or IDM credentials can sign in using their current account. [Continue](#)

FAQs
How do I know which [sign in option](#) to choose?
Why does this [sign in page](#) look different?

1. Click **Continue** on the EUA or IDM User ID option.

Figure 14: IDM Sign In/Create your CMS Account Page User ID and Password

Sign in/Create your CMS account

User ID

❗ This field cannot be left blank

Password

❗ This field cannot be left blank

[Sign in](#)

Having issues signing in?
Manage your IDM/EUA credentials at the links below.

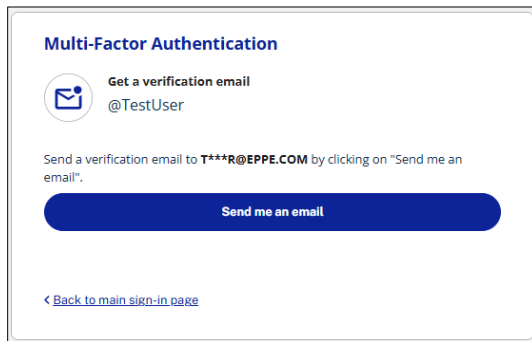
[Forgot IDM User ID](#) [EUA Login Form](#)
[Forgot IDM Password](#) [Forgot EUA Password](#)
[IDM User Registration](#)
[Unlock IDM Account](#)
[Help Center](#)

[Back to main sign-in page](#)

1. Enter **User ID** and **Password**.
2. Click **Sign In**.

The Multi-Factor Authentication page is displayed.

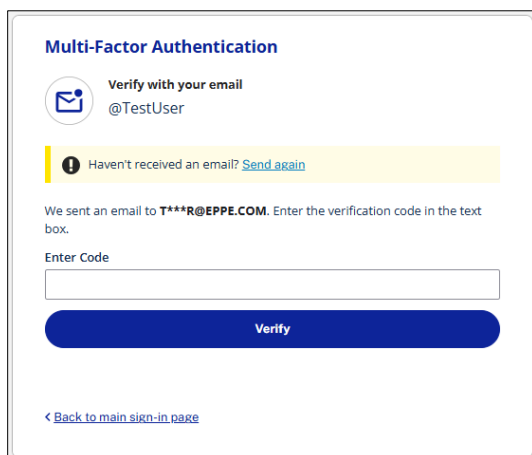
Figure 15: IDM Multi-Factor Authentication Request

The screenshot shows a web page titled "Multi-Factor Authentication". It features a blue header with the title. Below the header, there is a section with an envelope icon and the text "Get a verification email @TestUser". A paragraph of text explains that a verification email will be sent to "T***R@EPPE.COM" by clicking the "Send me an email" button. The button is a large, rounded blue rectangle. At the bottom left, there is a link that says "< Back to main sign-in page".

1. Click **Send me an email**

The Multi-Factor Authentication verification page is displayed

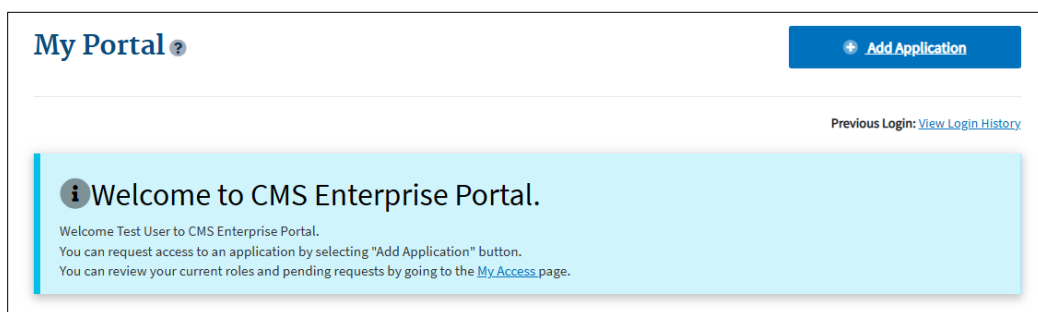
Figure 16: IDM Multi-Factor Authentication Request Enter Code

The screenshot shows a web page titled "Multi-Factor Authentication". It features a blue header with the title. Below the header, there is a section with an envelope icon and the text "Verify with your email @TestUser". A yellow warning box contains an information icon and the text "Haven't received an email? [Send again](#)". Below this, a paragraph of text explains that a verification code was sent to "T***R@EPPE.COM" and should be entered in the text box. The text box is labeled "Enter Code". Below the text box is a large, rounded blue button labeled "Verify". At the bottom left, there is a link that says "< Back to main sign-in page".

1. Enter **Code**.
2. Click **Verify**.

The My Portal page is displayed.

Figure 17: IDM My Portal Page

The screenshot shows a web page titled "My Portal". It features a blue header with the title and a blue button labeled "Add Application". Below the header, there is a section with a light blue background. It contains an information icon and the text "Welcome to CMS Enterprise Portal." followed by a paragraph of text: "Welcome Test User to CMS Enterprise Portal. You can request access to an application by selecting 'Add Application' button. You can review your current roles and pending requests by going to the [My Access](#) page." At the top right of the light blue section, there is a link that says "Previous Login: [View Login History](#)".

1. Select on **“Add Application”** to request access to the EPPE application.

The Request Application Access Page is displayed.

Figure 18: Requesting Access Role Selection

1. The **Select an Application** field is populated by default.
2. Select the **Select a Role** field and choose **EPPE User** from the dropdown menu.
3. Click **Next**.

Figure 19: Requesting Access Identity Verification

1. Click **Launch** to start the **Identity Verification** process.

2.5 Experian Identity Verification

The Experian identity verification service will use the user's core credentials to locate their personal information in Experian and generate a set of questions, referred to as out-of-wallet questions. Experian will attempt to verify their identity to the appropriate level of assurance with

the information they provided. Most users are able to complete the ID proofing process in less than five minutes. If users encounter problems with RIDP, they will be asked to contact Experian Support Services via phone to resolve any issues. The Experian identity verification is a required step to access the EPPE system and must be completed.

Users may have already encountered Remote Identity Proofing (RIDP) through various interactions with banking systems, credit reporting agencies, and shipping companies. The Experian identity verification service is used by CMS to confirm your identity when users access a protected CMS Application. When users log into the CMS system and request access to EPPE, they will be prompted to RIDP if they have not been previously identity proofed to the level of assurance required by the EPPE application. The RIDP will not impact the user's credit. Users will be asked to provide a set of core credentials which include:

1. Full Legal Name
2. Social Security Number
3. Date of Birth
4. Current Residential Address
5. Personal Phone Number

Figure 20: Identity Verification Step 1

Step #1: Identity Verification Overview

To protect your privacy, you will need to complete Identity Verification successfully, before requesting access to the selected role. Below are a few items to keep in mind.

1. Ensure that you have entered your legal name, current home address, phone number, date of birth and email address correctly. We will only collect personal information to verify your identity with Experian, an external Identity Verification provider.
2. Identity Verification involves Experian using information from your credit report to help confirm your identity. As a result, you may see an entry called a "soft inquiry" on your Experian credit report. Soft inquiries do not affect your credit score and you do not incur any charges related to them.
3. You may need to have access to your personal and credit report information, as the Experian application will pose questions to you, based on data in their files. For additional information, please see the Experian Consumer Assistance website - <http://www.experian.com/help/>

If you elect to proceed now, you will be prompted with a Terms and Conditions statement that explains how your Personal Identifiable Information (PII) is used to confirm your identity. To continue this process, select 'Next'.

Next Cancel

1. Click **Next**.

Figure 21: Identity Verification Step 2

Step #2: Accept Terms & Conditions

OMB No. 0938-1236 | Expiration Date: 04/30/2017 | (OMB Re-Certification Pending) | [Paperwork Reduction Act](#)

Protecting Your Privacy

Protecting your Privacy is a top priority at CMS. We are committed to ensuring the security and confidentiality of the user registering to EIDM. Please read the [CMS Privacy Act Statement](#), which describes how we use the information you provide.

Personal information is described as data that is unique to an individual, such as a name, address, telephone number, Social Security Number, and date of birth (DOB). CMS is very aware of the privacy concerns around PII data. In fact, we share your concerns. We will only collect personal information to verify your identity. Your information will be disclosed to Experian, an external authentication service provider, to help us verify your identity. If collected, we will validate your Social Security Number with Experian only for the purposes of verifying your identity. Experian verifies the information you give us against their records. We may also use your answers to the challenge questions and other PII to later identify you in case you forget or misplace your User ID / Password.

HHS Rules of Behavior

We encourage you to read the [HHS Rules of Behavior](#), which provides the appropriate use of all HHS information technology resources for Department users, including Federal employees, contractors, and other system users.

☒ I agree to the Terms & Conditions

Back **Next** Cancel

1. Click the **I agree to the Terms & Conditions** checkbox.
2. Click **Next**.

Figure 22: Identity Verification Step 3

Step #3: Enter Your Information

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

All fields are required unless marked 'optional'.

First Name: EPPE Middle Name (optional): Last Name: User Suffix (optional):

Social Security Number: ***** Birth Month: January Birth Date: 1 Birth Year: 1960

Is Your Address US Based? ☒ Yes ☐ No

Home Address Line 1: Home Address One Enter Home Address Line 2 (optional):

City: City State: Maryland ZIP Code: 21075 Enter ZIP+4 Code (optional):

Phone Number: 410-410-4100

Email Address: eppeuser1@eppe.com Confirm Email Address: eppeuser1@eppe.com

☒ Check here if you have read and verified the information above is accurate and complete as required by Identity Verification.

Back Next Cancel

1. Click the **Check here if you have read and verified the information above is accurate and complete as required by Identity Verification** checkbox.
2. Click **Next**.

Figure 23: Identity Verification Confirmation

Step #4: Verify Your Identity

Confirmation

You have successfully completed the Remote Identity Proofing process.

Next

1. The confirmation message, **"You have successfully completed the Remote Identity Proofing process"** displays.
2. Click **Next**.

2.6 Requesting Access to EPPE

Requesting Access to EPPE is accessible when the Identification Verification is complete.

Figure 24: Requesting Access Role Details

CMS.gov | My Enterprise Portal

Request Application Access

- Select an Application**
✓ EPPE
Completed [Edit](#)
- Select a Role**
✓ EPPE User
Completed [Edit](#)
- Complete Identity Verification**
✓ Identity Verification
Completed
- Enter Role Details**
All fields are required unless marked 'optional'.
Enter EPPE Organization Name
[Next](#)
- Enter Reason for Request**
[Cancel](#)

1. Enter the **Organization Name**.
2. Click **Next**.

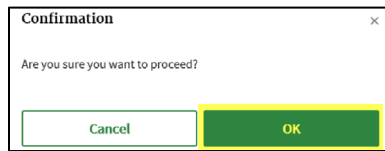
Figure 25: Requesting Access Reason for Request

CMS.gov | My Enterprise Portal

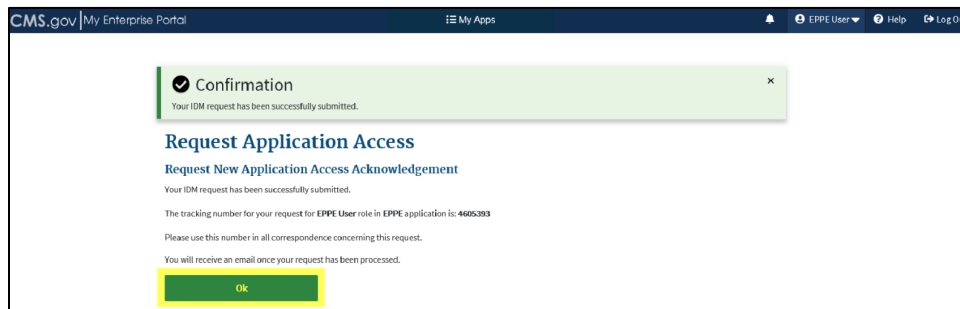
Request Application Access

- Select an Application**
✓ EPPE
Completed [Edit](#)
- Select a Role**
✓ EPPE User
Completed [Edit](#)
- Complete Identity Verification**
✓ Identity Verification
Completed
- Enter Role Details**
All fields are required unless marked 'optional'.
EPPE Organization Name
CMS
Completed [Edit](#)
- Enter Reason for Request**
Enter a Reason for Request
[Submit](#)
[Cancel](#)

1. Enter the **Reason for Request**.
2. Click **Submit**.

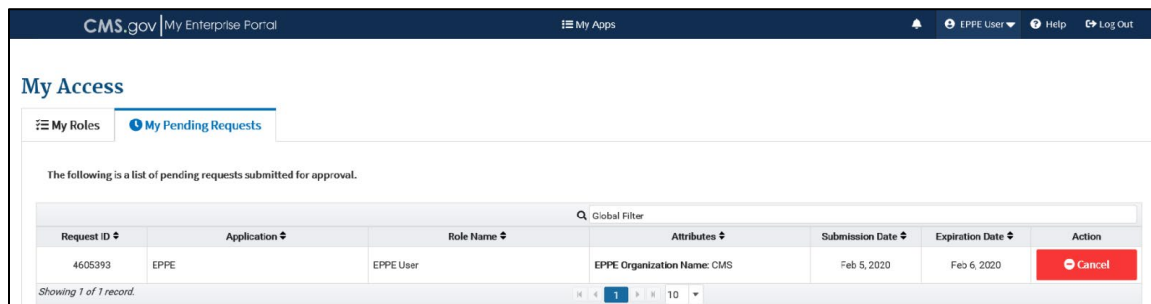
Figure 26: Requesting Access Confirmation Request

1. Click **OK** to proceed.

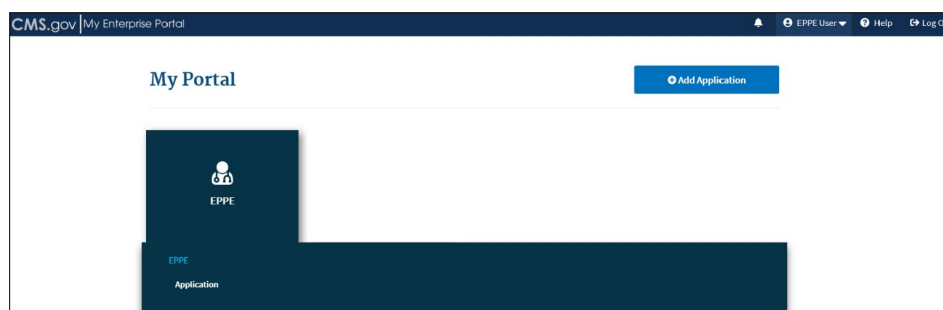
Figure 27: Requesting Access Confirmation Message

2. Click **Ok** to return to the Enterprise Portal page.

2.7 Requesting Access to EPPE Roles

Figure 28: Requesting Access My Access Page

At this point, the Application Access Request is complete. The request must be approved. An email will be sent once the pending request is approved. After access is granted, log into the Enterprise Portal.

Figure 29: Requesting an EPPE Role My Portal Page

1. Click the **EPPE** tile.
2. Then select on the **Application** link.

Figure 30: Requesting an EPPE Role EPPE First Time User Page

EPPE
Enterprise Privacy Policy Engine

USER GUIDES | CHARLIEBROWN

Welcome, Charlie Brown.
This is your first login.

Welcome to EPPE

Note: Our records indicate that you are a first-time user with EPPE or a user with no active role in EPPE. You must be associated with one or more organizations and be associated with one or more roles to use EPPE.

Select < [Request Role in EPPE](#) > if you wish to request a role and organization assignment.

If you have questions, please contact the EPPE help desk at 844-EPPE-4 (844-377-3382) or EPPE@cms.hhs.gov.

Request Role in EPPE

Your Pending Role Request(s)

ID	Organization	Requested Role	Date Requested	Actions
You do not have any pending role requests. Use the Request Role in EPPE button above to request a role.				

Displaying 0 - 0 of 0

1. Click the **Request a Role in EPPE** hyperlink or button.

The Request a Role in EPPE pop-out window is displayed.

Figure 31: Requesting an EPPE Role Request a Role in EPPE Pop-Out Window

Request Role in EPPE

Request Role in EPPE

Organization Name*

Please select your organization

[Cannot locate your Organization?](#)

Role*

Please select your organization first

Please select the appropriate role from available items.

Submit [Cancel](#)

2. Select an **Organization** from the dropdown menu.
3. Select a **Role** from the dropdown menu.
4. Click **Submit**.

Figure 32: EPPE Role Request Attestation.

Request Role In EPPE

Request Role In EPPE **Attestation**

Agreeing to this statement confirms that I have completed the mandatory training for the role that I am requesting, as specified on the [EPPE web page](#).

☐ I agree.*

Previous **Submit** Cancel

2. Click the **I agree** checkbox.

Figure 33: Requesting an EPPE Role Confirmation.

CMS.gov | My Enterprise Portal

EPPE
Enterprise Privacy Policy Engine

USER GUIDES CHARLIEBROWN

✓ Your role request for *DUA Requester* with *MARICOM SYSTEMS, INC.* has been submitted for review and approval. (reference number 20015)

⚠ **Welcome to EPPE**

Note: Our records indicate that you are a first-time user with EPPE or a user with no active role in EPPE. You must be associated with one or more organizations and be associated with one or more roles to use EPPE.

Select < Request Role in EPPE > if you wish to request a role and organization assignment.

If you have questions, please contact the EPPE help desk at 844-EPPE-DUA (844-377-3382) or EPPE@cms.hhs.gov.

Request Role in EPPE

Your Pending Role Request(s)

ID	Organization	Requested Role	Date Requested	Actions
20015	MARICOM SYSTEMS, INC.	DUA Requester	12/20/2023	Remove

Displaying 1 - 1 of 1

1. The EPPE role request submission acknowledgement displays the message, “**Your organization/role request has been submitted for approval.**”
2. The EPPE Administrator will review for approval.

3 Acronyms and Glossary

The following are acronyms used within the EPPE system.

Table 1: Acronyms

Acronym	Definition
CMS	Centers for Medicare and Medicaid Services
DUA	Data Use Agreement
EPPE	Enterprise Privacy Policy Engine
IDM	Identity Management
MFA	Multi-Factor Authentication
PDF	Portable Document Format

4 EPPE Help Desk Information

EPPE Help Desk Contact Information

Hours of Operation: Monday – Friday 9:00 AM to 6:00 PM EST

844-EPPE-DUA (844-377-3382)

eppe@cms.hhs.gov