Enterprise Privacy Policy Engine (EPPE)

Frequently Asked Questions

Date: April 14th, 2021 Version: 2.1

Contents

Identity Management (IDM)

IDM001 - What is IDM?

IDM is the acronym for CMS' Identity Management service, which includes Remote Identity Proofing, Access Management, Multi-Factor Authentication, Authorization Assistance Workflow Tools, and Identity Lifecycle Management functions (i.e., password reset, re-certification, forgotten User ID, etc.).

Back to Top

IDM002 - How can I access IDM?

To access the EPPE system you first have to register for a User ID and password for the Identity Management (IDM) system.

1. If you are accessing the CMS Enterprise Portal from the Internet, please navigate to https://portal.cms.gov. If you are accessing the CMS Enterprise Portal from the CMS Intranet, please navigate to https://portal.cms.cmsnet. The EUA User ID cannot be used in conjunction with the EPPE application. A new IDM User ID has to be created.
2. On the CMS Enterprise Portal page, select the **<New User Registration>** link.
3. In Step #1, select the appropriate application.
4. Read and agree to the Terms and Conditions by checking the box and clicking **<Next>** at the bottom of the page.
5. In Step #2, provide the information requested on the **<Register Your Information>** page and click **<Next>** at the bottom of the page.
6. Create a User ID, Password and Challenge Question on the **<Create User ID, Password & Security Question/Answer>** page and click <Next> at the bottom of the page.
7. Review the information on the **<New User Registration Summary>** page and click on **<Submit User>** on the bottom of the page. You will receive an email acknowledging your successful registration.

Back to Top

IDM003 - How can I view the IDM User Guide?

The following are step-by-step instructions on how to access the IDM User Guide.

1. Navigate to the portal link at https://portal.cms.gov.
2. Click on the **<Help>** link in the upper right-hand corner.
3. Under the heading **<User Manual>** click on the link **<Enterprise Portal User Manual>**.

Back to Top

IDM004 - How can I get my User ID if I forgot it?

The following are basic step-by-step instructions on how to use the **<Forgot User ID?>** feature.

1. Navigate to the CMS Enterprise Portal page at https://portal.cms.gov.
2. Select the **<Forgot User ID?>** link on the CMS Enterprise Portal.
3. Provide the information required on the **<Forgot User ID?>** page and select **<Submit>** to continue.
4. The acknowledgement page is displays and informs the user that the information entered has been successfully verified and an email, with your User ID, has been sent to the email address on record.

Back to Top

IDM005 - What should I do if I forget my password?

The following are basic step-by-step instructions on how to use the **<Forgot Password?>** feature to create a new password.

1. Navigate to https://portal.cms.gov.
2. Select the **<Forgot Password?>** link on the CMS Enterprise Portal page.
3. Enter your User ID and select **<Next>** to continue.
4. Select your Recovery Method.
5. Provide the answers to the challenge question.
6. Enter a password in the box**.**
7. Re-enter the same password for **<Enter Confirm Password>** and select **<Reset Password>**.
8. The acknowledgement page is displays and informs the user that the password has been successfully changed and an email has been sent to the email address on record.

Back to Top

IDM006 - How can I view my profile?

The following are basic step-by-step instructions on how to **<View My Profile>** information.

1. Navigate to https://portal.cms.gov.
2. After you are logged in, click on your name in the upper right-hand side of the CMS Enterprise Portal page.
3. Select **<My Profile>** from the dropdown menu to continue, and the **<My Profile>** page displays.

Back to Top

IDM007 - How can I change my password?

The following are basic step-by-step instructions on how to **<Change Your Password>**.

1. Navigate to https://portal.cms.gov.
2. After you are logged in, click on your name in the upper right-hand side of the CMS Enterprise Portal page.

3. Select **<My Profile>** from the dropdown menu to continue, and the **<My Profile>** page displays.
4. Select **<Change Password>** from the left-hand side, and the **<Change Password>** page displays.
5. Enter your old password in the **<Enter Old Password>** box.
6. Create and enter a new password of your choice for **<Enter New Password>.**
7. Re-enter the same password for **<Confirm New Password>** and select **<Submit>** to continue.
8. The **<Change Password>** is acknowledged and the portal returns to the login page.

Back to Top

IDM008 - How can I change my email address?

The following are basic step-by-step instructions on how to **<Change Email Address>**.

1. Navigate to https://portal.cms.gov.
2. After you are logged in, click on your name in the upper right-hand side of the CMS Enterprise Portal page.
3. Select **<My Profile>** from the dropdown menu to continue, and the **<My Profile>** page displays.
4. Select **<Change Profile>** the left-hand side, and the **<Change Profile>** page displays.
5. Scroll to the **<Email Address>** and provide your new email address.
6. Provide the same email address in the **<Confirm Email Address>** box.
7. Scroll to the bottom of the page and click on **<Submit>**.
8. The email address change is confirmed and the **<View My Profile>** displays.

Back to Top

IDM009 - How can I change my security challenge question and answer?

The following are basic step-by-step instructions on how to use the **<Change Security Question>** feature.

1. Navigate to https://portal.cms.gov.
2. After you are logged in, click on your name in the upper right-hand side of the CMS Enterprise Portal page.
3. Select **<My Profile>** from the dropdown menu to continue, and the **<My Profile>** page displays.
4. Select **<Change Security Question>** from the left-hand side, and the **<Change Profile>** page displays.
5. Pick from the **<Select Your Security Question>** dropdown list.
6. Provide the answer of your choosing in the **<Enter Security Answer>** box.
7. Select **<Submit>** to continue.
8. The change to the challenge questions is confirmed and the **<View My Profile>** displays.

Back to Top

IDM010 - How can I change my phone number?

The following are basic step-by-step instructions on how to **<Change Phone Number>** feature.

1. Navigate to https://portal.cms.gov.
2. After you are logged in, click on your name in the upper right-hand side of the CMS Enterprise Portal page.
3. Select **<My Profile>** from the dropdown menu to continue, and the **<My Profile>** page displays.
4. Select **<Change Profile>** the left-hand side, and the **<Change Profile>** page displays.
5. Scroll to the **<Phone Number>** and provide your new phone number.
6. Scroll to the bottom of the page and click on **<Submit>**.
7. The phone number change is confirmed and the **<View My Profile>** displays.

Back to Top

IDM011 - How can I change my home address?

The following are basic step-by-step instructions on how to **<Change Home Address>** feature.

1. Navigate to https://portal.cms.gov.
2. After you are logged in, click on your name in the upper right-hand side of the CMS Enterprise Portal page.
3. Select **<My Profile>** from the dropdown menu to continue, and the **<My Profile>** page displays.
4. Select **<Change Profile>** the left-hand side, and the **<Change Profile>** page displays.
5. Scroll to the address boxes and provide your new home address.
6. Scroll to the bottom of the page and click on **<Submit>**.

7. The home address change is confirmed and the **<View My Profile>** displays.

Back to Top

IDM012 - When I try to login, I get an error message stating, "Your information cannot be verified. Please try again." What should I do?

Please check the User ID and password that you entered. An incorrect combination of these will result in such an error message.

Back to Top

IDM013 - When I try to login, I get the error message stating, "Your account is disabled. Contact the Help Desk to enable your account." Why does this happen?

A user's account can be disabled by application help desks or IDM Administrators for possible reasons linked to security violations or fraud detection. In order to enable your disabled account, you are required to contact the application helpdesk.

Back to Top

IDM014 - When I try to login, I get the error message stating, "Your account has been locked. Please try again later." Why did this happen and how can I get my account unlocked?

After three unsuccessful attempts to login, your account will be locked. Your account will be unlocked after 60 minutes have elapsed since your third consecutive failed authentication attempt. You are required to enter valid credentials associated with your user account to unlock the account.

Back to Top

IDM015 - When I try to login, I am directed to the 'Unlock My Account' view. Why is this and how do I unlock my account?

IDM locks your user account if no account activity is reported for 60 days. When you login after 60 days the system will display the 'Unlock my Account' view; enter your **<User ID>** and correctly answer the challenge question on the next page; enter your new password in the input fields of **<Enter New Password>** and **<Confirm New Password>** to unlock your account.

Back to Top

IDM016 - Why do I need to answer a challenge question when unlocking my user account?

IDM needs to verify your identity. Your response to the challenge question will enable IDM to confirm your identity and help you proceed in getting your account unlocked. This also protects you from identity theft.

Back to Top

IDM017 - Who is eligible to have a CMS IDM User Account?

All U.S. citizens who are over 18 years of age and have a current or previous valid U.S. residential address are eligible to have a CMS IDM User Account.

Back to Top

IDM018 - What is an IDM User account?

IDM is an acronym for Identity Management. An IDM account verifies the identity of the user and ensures that only authorized/registered users can access protected information and systems through the CMS Enterprise Portal.

Back to Top

IDM019 - I am new to the CMS Enterprise Portal; how should I create my user account?

Once you are on the CMS enterprise portal at https://portal.cms.gov, select the **<New User Registration>** link. You are required to enter a combination of your business and personal information and select and answer a Security Questions. Choose desired User ID / Password as per the guidelines provided. Once the details have been successfully updated in IDM, the system will display a message confirming the creation of the user account.

Back to Top

IDM020 - Why should I submit personal information at the time of registering my user account, and how safe is it?

IDM needs your personal information to verify your identity. During the registration process, IDM initiates a Remote Identity Proofing (RIDP) call with one of the identity service providers and based upon the information provided, allows you to create a user account.

For security level information please visit: http://www.cms.gov/About-CMS/Agency-Information/Aboutwebsite/Privacy-Policy.html

Back to Top

IDM021 - What will you do with my personally identifiable information?

IDM uses an external authentication service provider, Experian, to help us verify your identity based on the information that you have provided. Experian verifies your information against its records to successfully identify you.

CMS provides, on the public-facing Web sites, the Terms & Conditions of how your information will be handled when registering for a CMS IDM user account.

Back to Top

IDM022 - Will my Social Security Number (SSN) be shared with any federal or private agency?

Your SSN will be shared with Experian, the authentication service provider, to verify your identity. IDM does not share your SSN with any other federal or private agency.

Back to Top

IDM023 - How long does my information stay with Experian?

Experian will only keep the information we share for seven years as required by federal laws, regulations, or guidelines.

Back to Top

IDM024 - Why does Experian require my personal information?

Experian may use credit information to help verify your identity; this may result in what is known as a "soft inquiry" on your Experian credit report.

Back to Top

IDM025 - Does verifying my identity by Experian affect my credit score?

No, your credit score is not affected. These kinds of inquiries are termed as "soft inquiry."

Soft inquiries:

- Do not affect your credit score, and you do not incur any charges related to them.
- Are displayed in the version of the credit profile viewable only to consumers and are not reported to lenders.

If you order a credit report from Experian, you will see an entry of inquiry by the Centers for Medicare & Medicaid Services with our address and the date of request.

Back to Top

IDM026 - What if I have problems? Is there an Experian Help Desk?

Yes, Experian Help Desk is a dedicated call center for individuals who have failed being proofed online while attempting to obtain a CMS IDM credential. The Experian Help Desk can be contacted at 1-866-578-5409. The Experian Help Desk is open Monday through Friday from 8:30 a.m. to 10:00 p.m., Saturday from 10:00 a.m. to 8:00 p.m., and Sunday from 11:00 a.m. to 8:00 p.m., Eastern Standard Time. Note: Sometimes it could take 24 hours before the verification will be recognized with the IDM system.

Back to Top

IDM027 - What happens if the Experian Help Desk cannot proof my identity?

If you contact the Experian Help Desk and your identity cannot be verified, you will need to contact the respective application help desk to complete the manual identity proofing process. Even though the manual identity proofing process was used to verify you, the application help desk still requires your Social Security Number (SSN).

Back to Top

IDM028 - Why am I unable to change my User ID?

The User ID identifies you uniquely to IDM; therefore, you cannot change your User ID.

Back to Top

IDM029 - How long does it take to get approved for access to a requested application or role?

It can take up to 30 days to be granted access to an application or role. After 30 days, your request will expire. In the unlikely event that this happens, please contact the respective application help desk.

Back to Top

IDM030 - What is Remote Identity Proofing (RIDP)?

RIDP is the process of validating sufficient information about you (e.g., credit history, personal demographic information, and other indicators) to uniquely identify you. If you are requesting electronic access to protected CMS information or systems, you must be identity proofed to gain access. CMS uses Experian, an external identification verification provider, to remotely perform identity proofing.

You may have already encountered 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 you need to access a protected CMS Application. When you log into the CMS system and request access to EPPE, you will be prompted to RIDP if you have not been previously identity proofed to the level of assurance required by the EPPE. You will be asked to provide a set of core credentials that include:

- Full Legal Name
- Social Security Number (may be optional)

- Date of Birth
- Current Residential Address
- Personal Phone Number

The Experian identity verification service will use your core credentials to locate your personal information in Experian and generate a set of questions, referred to as out-of-wallet questions. Experian will attempt to verify your identity to the appropriate level of assurance with the information you provided. Most users are able to complete the ID proofing process in less than five minutes. If you encounter problems with RIDP, you will be asked to contact Experian Support Services via phone to resolve any issues.

Back to Top

IDM031 - Where can I find information on who has the right to request an SSN?

Specific laws require a person to provide his or her SSN for certain purposes. Federal law mandates that state Departments of Motor Vehicles, tax authorities, welfare offices, and other governmental agencies request your SSN as proof that you are who you claim to be. However, the Privacy Act of 1974 requires that government agencies at the local, state, and federal level disclose to each person whether submitting your Social Security number is required, details on the use of this information, and what law or authority requires its use.

For information on who has the right to request your SSN, please see link below:
http://www.identityhawk.com/Who-Can-Lawfully-Request-My-Social-Security-Number

The text of the Privacy Act can be found at http://www.justice.gov/opcl/privstat.htm

Back to Top

IDM032 - What happens to the data submitted for identity proofing?

IDM collects personal information only to verify your identity. Your information will be sent to Experian, an external identity verification provider, to help us confirm your identity. Experian verifies the information you give us against their records and may present you with questions based on your credit profile, called out-of-wallet questions. The out-of-wallet questions and answers, including financial history, are strictly between you and Experian; neither the EPPE application nor CMS can access or store this information. For more information regarding how CMS uses the information you provide, please read the CMS Privacy Act Statement.

Back to Top

IDM033 - I already provided my personal information during registration to setup an IDM user account. Why do I have to provide it again to access certain applications?

When you have selected an application or role that requires a higher level of security, you are required to complete identity verification. In most cases, you may need to provide a few more details (i.e. SSN, Date of Birth) to be able to request access to the selected application or role.

Back to Top

IDM034 - What happens if my identity cannot be verified during the online Remote Identity Proofing process?

If Experian cannot identity proof you online, you will be asked to contact either the Experian Verification Support Services Help Desk or the respective application help desk, depending on the reason you failed RIDP. The system will provide you with a reference number to track your case. The Experian Help Desk cannot assist you if you do not have the reference number. If you are asked to contact the application help desk, you will be given a ticket number to help the application help desk perform the manual identity proofing process with you. Even though the manual identity proofing process was used to verify you, the application help desk still requires your Social Security Number (SSN).

Back to Top

IDM035 - Why do I need to provide my SSN?

The Identity Management (IDM) system is a public government website, allowing any U.S. citizen over the age of 18 to open an account. IDM is designed to use your SSN to verify your identity. Since you are applying for access to a Federal application that is housed behind the IDM portal, your SSN is required to complete the verification.

Back to Top

IDM036 - Why am I getting an access denied message when requesting access to the EPPE application?

You might be attempting to log into the CMS Enterprise Portal with an incorrect User ID. The CMS Enterprise Portal User ID is created when first setting up your portal account and is not used by any other CMS system (such as EUA). If you do not have an account on the CMS Enterprise Portal, you will first need to set one up before accessing EPPE. This process can be started by clicking the "New User Registration" button located on the login screen at https://portal.cms.gov/wps/portal/unauthportal/home/.

Back to Top

IDM037 – How does the EIDM to IDM migration affect users?

On February 15th, the Symantec VIP software currently used by EPPE for multi-factor authentication (MFA) is being eliminated. This change is part of a transition to a new identity management system for the CMS Portal, which hosts EPPE.

Instead of using Symantec VIP, you will have several MFA options to choose from to access EPPE. Your new MFA options are:

- Email – This is the default option that will be used to access EPPE the first time you login after February 15th. The email option will send your security code to your email address. Once you login successfully, you can add any of the other MFA options through a profile update. The email option cannot be removed, and it is the only option that will always remain on your profile. However, we recommend that you select an additional MFA option in case email is experiencing a temporary delay.
- Short Message Service (SMS) – The SMS option will send your security 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 security 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, if needed, an extension).
- Google Authenticator – Google Authenticator is an application for your smart phone that generates security codes. Supported phones include iPhone, Android Phone, and Blackberry (a download to your smartphone is required).
- Okta Verify – Okta Verify is an application for your smart phone that produces push notifications which allow you to verify your identity with a single tap on your device, without the need to type a security code. Supported phones include iPhone, Android Phone, and Windows Phone (a download to user's smartphone is required).

You will also experience a new login process flow after February 15th. The new login process will be on two pages. The initial page will ask for your User ID and Password. The second page will handle the MFA verification.

Back to Top

EPPE Registration (ER)

ER001 - How can I access EPPE?

To request access to the EPPE application and a role follow the instructions below.

1. If you already have a User ID and password, navigate to https://portal.cms.gov. If you do not have a User ID, please refer to FAQ IDM002.
2. Log in with your User ID and password.
3. On the **<My Portal>** click on **<Add Application>**.
4. After the **<Request Application Access>** page is displayed, select **"EPPE"** from the **<Select an Application>** dropdown list and click on **<Next>**.
5. Select the **"EPPE User"** role from the **<Select a Role>** dropdown list and click on **<Next>.**
6. Click on **<Complete Identity Verification>** and then **<Launch>**.
7. Follow the instructions on the Identity Verification pages and select the appropriate information needed to complete your request for access (IDM will prompt on what is needed).
8. Click on **<Enter Role Details>** and provide the **<EPPE Organization Name>.** The organization's name must reflect the organization the user is currently associated with.
9. Click on the **<Enter Reason for Request>** field and provide a short justification for this access request.
10. Click on **<Submit>**.

Back to Top

ER002 - I was already approved for EPPE access, why am I being asked to request a role again?

EPPE requires a two-step approval process. The first approval grants you access to the EPPE application as an EPPE User. The second approval is for a specific role within the EPPE application (i.e., COR or DUA Requester roles).

Back to Top

ER003 - How long does it take for my role to be approved within the EPPE system?

Approvals are handled by the EPPE Administrator. Generally, they are processed within 1 - 2 business days. You will receive an email notifying you when the Administrator approves your role.

Back to Top

Multi-Factor Authentication (MFA)

MFA001 - What is Multi-Factor Authentication?

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

- 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).
- The third factor is who users are, as indicated by some biometric characteristic, such as a fingerprint or an iris pattern.

Two-factor authentication means that instead of using only one single type of authentication token or factor, such as only things a user knows (passwords, shared secrets, solicited personal information, etc.), a second token or factor, something the user has or something the user is, must also be supplied in order to complete the authentication process.

Back to Top

MFA002 - Why is there a long delay receiving the MFA Security Code email?

The email may be delayed by a firewall or virus scans. To bypass this issue, you can register other MFA devices to your profile.

Back to Top

MFA003 - How do I use my Multi-Factor Authentication device to Log into my CMS IDM User account?

Once you have received the email with the 6-digit security code, you must enter it in the **<MFA Code is required>** field and click on **<Verify>**.

Back to Top

MFA004 - How do I add my Multi-Factor Authentication device to my CMS IDM User Account?

You add the Multi-Factor Authentication device by selecting your MFA Device Type from the dropdown list after entering your password.

Back to Top

MFA005 - Why is Multi-Factor Authorization required?

As more and more information is made available and transacted online, new and improved processes and technologies are required to assure that individuals are provided appropriate access to information and only the access that they are authorized to have. This type of authentication security is being used for many online systems across industries that require this greater level of assurance. These systems also support the government's initiatives, leveraging the same technology, for a safer and secure Internet in which a common online identity can be used.

Back to Top

MFA006 - How do I use Multi-Factor Authentication?

When logging into the system, the individual will be asked to enter their username, password and then a one-time security code that is generated and emailed to the user. This onetime security code can be generated by one of several media that are available. The onetime security code can be generated by an email or an application that needs to be downloaded to your smartphone or received via an SMS or voice phone call if your phone is properly registered.

Back to Top

MFA007 - What mobile devices are supported?

Google Authenticator is supported on the iPhone, Android Phone, and Blackberry. Okta Verify is supported on the iPhone, Android Phone, and Windows Phone. Both Apps (Google Authenticator and Okta Verify) require an app download to your mobile device.

Back to Top

MFA008 - Will I be charged mobile device data rates each time I use Google Authenticator or Okta Verify on my mobile device?

No, you will not be charged. Once the Google Authenticator or the Okta Verify MFA application is loaded onto your mobile device, it does not utilize any data usage. Cell or network traffic is used to download the application to one's mobile device.

Back to Top

MFA009 - How do I download the MFA software on a mobile device?

For the different mobile devices refer to the links or applicable app stores. Search for Google Authenticator and/or Okta Verify.

- iOS (iPhone, iPad) – Go to the App Store.
- Android – Go to the Play Store within Apps.
- Blackberry – Go to the BlackBerry World.
- Windows Mobile - Go to the Marketplace.

Back to Top

MFA010 - Why can't I use the desktop software or the mobile phone software?

An option is available to use a voice or SMS based soft token delivery method. This would require that you provide a phone number to receive either a phone call or text message. When that number is registered with IDM you will be presented with the option to receive a phone-based token delivery during your login process. Upon requesting token delivery, you will receive either a phone call or text message with your six-digit one-time password.

These SMS and voice tokens expire within 1 hour of when they are sent to a user. Please make sure you provide a phone number that will be accessible to you during your typical work hours, i.e., do not use a residential phone number if you will normally login from your place of employment.

Back to Top

EPPE Roles (ERO)

ERO001 - Who is a DUA Requester?

A DUA requester is a person authorized to legally bind their organization to the terms specified in the Data Use Agreement (DUA). This is a required role on the DUA.

Back to Top

ERO002 - Who is a Custodian?

Custodians are individuals who will have actual possession of the CMS data files, and who will be responsible for observance of all conditions of use, including the establishment and maintenance of security arrangements to prevent unauthorized use. This is a required role on the DUA and in rare instances may be the same individual as the Requester.

Back to Top

ERO003 - Who is a CMS Contracting Officer's Representative (COR)?

A COR is an employee of CMS responsible for ensuring that their contractors meet the commitments of their contracts.

Back to Top

ERO004 - Who are the Data Use Agreement (DUA) Management Team?

The DUA Team are within the Data and Information Dissemination Group/Office of Enterprise Data & Analytics at CMS and are responsible for overseeing the EPPE system and the tracking of CMS disclosures of PII/PHI.

Back to Top

ERO005 - Who is an EPPE Administrator?

An EPPE Administrator is a member of the Data and Information Dissemination Group/Office of Enterprise Data & Analytics at CMS, who is responsible for approving roles, changing reference data, and making high-level decisions in EPPE.

Back to Top

ERO006 - Who is an Extractor?

An employee or contractor of CMS responsible for gathering the specific data indicated in the Data Use Agreement (DUA) for dissemination to the requesting entity.

Back to Top

ERO007 - Who is a Shipper?

An employee or contractor of CMS responsible for the physical and/or digital delivery of the requested data files to the requesting entity.

Back to Top

ERO008 - How do I request a role in the EPPE system?

Once your access to the EPPE system has been approved, you will need to log into EPPE. On the EPPE Welcome page there will be a blue link **<Request Access>**. Click on the blue link to start the EPPE role request process.

Back to Top

ERO009 - Is it possible to request multiple roles on the EPPE system?

Yes, you can request multiple roles in the EPPE system. During the initial request, you can continue to add additional roles to the “Your Selection” portion of the screen. Once all necessary roles are requested, click on **<Submit>**. Users can also request additional roles at any time from the “Request Additional Role” option under the “My Organizations” tab.

Back to Top

ERO010 - How can I switch between roles?

To switch roles, click on the **<Switch To>** dropdown list in the upper right-hand side and choose the appropriate role to activate.

Back to Top

ERO011 - How do I remove EPPE access and make role(s) inactive for my organization?

To remove your access or make your role(s) inactive in the EPPE application, please submit a request to the EPPE Help Desk at EPPE@cms.hhs.gov . If you are making the request on behalf of another user associated with your company, the user’s supervisor would need to email the request to remove the access to the EPPE Help Desk. Once completed, the EPPE Help Desk will confirm that the access has been removed.

Back to Top

EPPE General Questions (EGQ)

EGQ001 - What is 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 user requesters and all CMS approvers can interactively use the system to manage the workflow. For those requests that require supporting documentation, it allows documents to be uploaded and then later downloaded for review.

Back to Top

EGQ002 - Why am I unable to do anything when I access EPPE?

Did you receive a message that your organization has an expired Data Use Agreement (DUA)? If you have an expired DUA the only DUA functions, you may perform are to extend or close the expired DUA. Until the expired DUA is extended or closed, you will not be allowed to do anything else in the EPPE system.

Back to Top

EGQ003 - Why is my organization suspended?

An organization is suspended if it has one or more expired Data Use Agreements (DUAs) that have not been remedied (either extended or closed). Any organization that has an expired CMS DUA will not receive authorization to obtain any new data until their expired DUA has been resolved.

Back to Top

EGQ004 - I receive a ton of EPPE email notifications. Can I turn off notifications?

On the bottom left-hand side of the menu items you will find **<My Preference(s)>**. Within that there is a link for **<Email Preference>**. Once you click on the link you will be able to disable or enable email notifications. Even if you disable email notifications, you will still receive email notifications for certain DUA actions that are required.

Back to Top

EGQ005 - Why didn't my DUA status switch to "Closed?"

All data files on the DUA **<DUA Number>** must be closed in order for the DUA to have a status of "Closed." If all the data files on the DUA selected to be closed are not closed, the DUA status will reflect "Open."

Back to Top

EGQ006 - How can I request an additional role?

On the navigation menu, under the **<My Access>** tab, click on **<Request Additional Role>**.

Back to Top

EGQ007 - How can I change my email preferences?

On the navigation menu, under the **<My Preference(s)>** tab, click on **<Email Preferences>**.

Back to Top

EGQ008 - How do I log out of EPPE?

On the navigation menu click on the **<Exit EPPE>** tab or click **<Log Out>** in the upper right-hand corner to log out of EPPE.

Back to Top

EGQ009 - How do I contact the EPPE Help Desk?

You may contact the EPPE Help Desk via phone at 844-EPPE-DUA (844-377-3382) or via email at eppe@cms.hhs.gov. The EPPE Help Desk operating hours are Monday through Friday 9 AM through 6 PM (EST).

Back to Top

EGQ010 - What are the file types that can be uploaded into EPPE?

The application will accept .doc, .xlsx, .pdf, and .txt files that are 2 MB or smaller. If the file type is invalid, the user will receive an error message and the file will not be uploaded successfully.

Back to Top

EGQ011 - Do I need to enter any job codes to request access to EPPE?

No. To access EPPE, users must have current IDM credentials to request access to the EPPE application. Once access is granted, the user must request a specific role for the EPPE application e.g. CMS Contact (COR) or DUA Requester.

Back to Top

EGQ012 - What does the data extraction percentage mean?

The data extraction percentage indicates the number of records provided for a specific file.

Back to Top

EGQ013 - How can we re-use data files if additional year(s) are needed and how can we utilize the “Apply-all” feature when adding new year(s)?

You may use the re-use feature for years of data that you currently have on other active DUAs. If you also need additional years of data for the file, you would have to request the new year(s) under a new file on the DUA. The “Apply-all” feature works for the new files listed on the DUA, but it will not work for the re-use files.

Back to Top

Modify Your DUA (MYD)

MYD001 - What is a DUA?

The Centers for Medicare & Medicaid Services (CMS) makes data files available to certain stakeholders as allowed by federal laws and regulations as well as CMS policy. CMS enters into Data Use Agreements (DUAs) with most data requesters for disclosures of protected health information (PHI) and/or personally identifiable information (PII) to ensure that data requesters adhere to CMS privacy and security requirements and data release policies.

Back to Top

MYD002 - I receive a ton of EPPE email notifications. Can I turn off notifications?

On the bottom left-hand side of the menu items you will find **<My Preference(s)>**. Within that there is a link for **<Email Preference>**. Once you click on the link you will be able to disable or enable email notifications. Even if you disable email notifications, you will still receive emails notifying you that certain actions are required of you on a DUA(s).

Back to Top

MYD003 - Why didn't my DUA status switch to "Closed?"

All data files on the DUA **<DUA Number>** must be closed in order for the DUA to have a status of "Closed." If all the data files on the DUA selected to be closed are not closed, the DUA status will reflect "Open."

Back to Top

MYD004 - My DUA expired. Why can't I find it immediately after extending it?

After a requester extends a Contractor DUA, it is routed to the COR, listed on the DUA, for the approval of the extension. Once the extension is approved, the requester will be able to find it in the Approval queue and the Contractor DUA is available for updates.

After a requester extends an LDS DUA, the DUA immediately shows in the Approval queue and is available for updates.

Back to Top

MYD005 - How can I search for a DUA?

On the navigation menu, under the Search tab, click DUA Search to pull up the search functionality.

Back to Top

MYD006 - Where can I find the recipient information on a DUA?

The recipient information is part of the data file attributes. The below steps will assist you in finding the recipient information.

1. Click on DUA Search.
2. Enter DUA# in the DUA Number field and click on Search.
3. Once the DUA displays in the search result screen, click on View.
4. When the DUA displays, scroll down to the data file section.
5. Click on the radio button next to each file to expand the file attributes.
6. The recipient information is part of the expanded data.

Back to Top

MYD007 - How can I contact the DUA Management Team?

You may contact the DUA Management Team via email at datauseagreement@cms.hhs.gov.

Back to Top

COR (COR)

COR001 - As a COR, why can't I see my DUAs in any of my queues?

DUAs will appear in your queues when you have actions to approve or deny. As a COR you may view all of your DUAs through the DUA search function.

Back to Top

COR002 - At the Proxy end date, will the COR or DUA Requester need to go in and end the Proxy assignment or will the system automatically end the assignment?

The system will automatically end the COR or Requester Proxy assignment at the end of the specified end date.

Back to Top

COR003 - How can the COR identify updates on the DUA?

The COR can identify updates on a DUA by accessing the DUA lifecycle. When the DUA lifecycle is expanded it will display and track the updates made on the DUA. A DUA Requester can enter comments detailing the updated information which will also display in the lifecycle.

Back to Top

COR004 - How do I get a list of my DUAs?

The DUA Requester and CORs can use the DUA Search function to review/export a list of DUAs to Excel.

Back to Top

COR005 - How can a COR access a previously approved DUA?

The COR that is listed on specific DUA(s) can access these DUAs through the DUA Search. The COR can search by a specific DUA number, status or various other attributes to view DUA(s).

Back to Top

COR006 - If the existing COR needs to be changed, will that COR need to approve the COR change?

Once the existing COR is changed on the DUA, the new COR will receive the update to approve. After the DUA update is approved by the new COR, it will then go to the DUA Management Team (DMT) for certification.

Back to Top

COR007 - Does the COR receive notifications from EPPE about DUA Change Contact requests?

The COR will receive a notification if a Change Contact Request lists them as the COR on the DUA.

Back to Top

Requester (REQ)

REQ001 - As a Requester on a CMS DUA, why am I unable to request or assign certain DUAs through the Change Contact function?

For a Requester from a CMS contractor to work with a DUA, the COR listed on the DUA needs to be active in the EPPE application. If the COR listed on the DUA does not have a role in EPPE yet, the application will display a message informing you that the COR is not registered. Please reach out to the COR and encourage them to register in the EPPE application. Once the COR is in the system, you will be able to request or assign the DUA through the Change Contact function.

Back to Top

REQ002 - How can the DUA Requester update the COR on a Contractor DUA?

The DUA Requester can update the COR on any Contractor DUA through the Update/Amend action.

Back to Top

REQ003 - What would happen with the DUA if both the DUA Requester and COR are no longer active?

If there is no one to register in IDM to request the role as the DUA Requester, a point of contact from the DUA's organization would need to email the DUA Management Team (DMT) at datauseagreement@cms.hhs.gov for assistance.

Back to Top

REQ004 - Should the DUA Requester create a DUA for each year of a contract Period of Performance (PoP)?

The DUA Requester should create a single DUA for the entire contract Period of Performance (POP). The DUA will need to be extended every year within the contract period.

Back to Top

REQ005 - Once a Contractor DUA is submitted, does is go to the COR for approval?

Yes, when the DUA is submitted by the DUA Requester, it is then waiting for the COR that is listed on the DUA to approve it. The COR will receive an email notification for pending DUA action(s).

Back to Top

REQ006 - Will there be any email notifications when a DUA is expiring?

Yes, the COR, DUA Requester and Custodians will receive an email notification. Email notifications are sent at 60 days, 30 days, 15 days and everyday thereafter until the DUA is either extended or closed.

Back to Top

REQ007 - At the Proxy end date, will the COR or DUA Requester need to go in and end the Proxy assignment or will the system automatically end the assignment?

The system will automatically end the COR or Requester Proxy assignment at the end of the specified end date.

Back to Top

REQ008 - When will OEDA stop accepting paper DUA forms?

OEDA will no longer accept DUA forms for Contractor or LDS DUAs through the datauseagreement@cms.hhs.gov mailbox. You can still submit paper DUA forms and updates for Research DUAs via the mailbox (DataUseAgreement@cms.hhs.gov).

Back to Top

REQ009 - Do you have to be a DUA Requester to be designated as a Proxy?

Yes, you must be registered as a DUA Requester before you can be selected by another DUA Requester as a DUA Requester Proxy.

Back to Top

REQ010 - How do I get a list of my DUAs?

The DUA Requester and CORs can use the DUA Search function to review/export a list of your DUAs to Excel.

Back to Top

REQ011 - When would the DUA Requester use the Ad Hoc Request?

A DUA Requester would utilize the Ad Hoc Request function if they are requesting assignment of a DUA from an outside organization. If the DUA Requester is associated with or was previously associated to another organization and does not see their DUA, they can request for the assignment of the DUA to themselves through the Ad Hoc request process, which will need EPPE Admin approval.

Back to Top

REQ012 - How are documents provided by the DUA Requester? Do they need to scan and send them via email?

The DUA Requesters will now have the ability to upload supporting documentation via the EPPE application. These documents are downloadable for viewing by both the COR and DUA Management Team (DMT).

Back to Top

REQ013 - If the existing COR needs to be changed, will that COR need to approve the COR change?

Once the existing COR is changed on the DUA, the new COR will receive the update to approve. After the DUA update is approved by the new COR, it will then go to the DUA Management Team (DMT) for certification.

Back to Top

REQ014 - What is the guidance on adding sub-contractors to the DUA?

If the contract holder is working with any sub-contractors, then the sub-contracting organizations should be listed on the DUA. If individuals from the sub-contracting organizations will be receiving data directly from CMS or accessing data through a CMS system, then they should also be listed as custodians on the DUA.

Back to Top

REQ015 - Does the CEO of a company have to be the DUA Requester on the DUA?

No. A DUA Requester is defined as “The person authorized to legally bind their organization to the terms specified in the DUA. This is a required role on the Data Use Agreement (DUA).”

Back to Top

REQ016 - What is a Data Extract System (DESY) User? Do we have to add these users?

A Data Extract System (DESY) User is not a user role within EPPE but rather users who need access to data files within the DESY data dissemination system. If a custodian will be accessing files directly through DESY, their 4-digit EUA ID will need to be provided in EPPE.

Back to Top

Extractor (EXT)

EXT001 - As an Extractor, how can I track partially extracted orders within EPPE?

That functionality does not currently exist in EPPE. The extractor has to manually track partial orders.

Back to Top

EXT002 - As an Extractor, how can I create an order?

On the extractor navigation menu, under the **<Order(s)>** tab, click on **<Create Orders(s)>** to create a new order.

Back to Top

EXT003 - As an Extractor, where can I view unfinished orders?

On the extractor navigation menu, under the **<Order(s)>** tab, click on **<Unfinished Order(s)>** to see unfinished orders.

Back to Top

EXT004 - As an Extractor, where can I view finished orders that haven't been shipped?

On the extractor navigation menu, under the **<Order(s)>** tab, click on **<Finished Order(s)>** to see orders extracted but not shipped.

Back to Top

EXT005 - As an Extractor, where can I view orders that have been shipped?

On the extractor navigation menu, under the **<Order(s)>** tab, click on to see orders that have been shipped.

Back to Top

Shipper (SHP)

SHP001 - As a Shipper, where can I view orders that are ready to be shipped?

On the shipper navigation menu, under the **<Shipping>** tab, click **<Pending Order(s)>** to see orders that are waiting for processing to be shipped.

Back to Top

SHP002 -As a Shipper, where can I view orders that have been shipped?

On the shipper navigation menu under the **<Shipping>** tab click **<Shipped Orders(s)>** to see orders that have been shipped.

Back to Top

MicroStrategy Reports (MSR)

MSR001 - How do I gain access to MicroStrategy Reports within EPPE?

If you require access to custom reports created for you by the EPPE team, you will need to get the **<MicroStrategy User>** role in order to view them. To request access to the MicroStrategy Reports within EPPE follow the steps outlined below.

1. If you already have a User ID and password, navigate to https://portal.cms.gov.
2. Log in with your User ID and password.
3. On the **<My Portal>** page, click on your name in the upper right-hand corner. Select **<My Access>**.
4. On any of your existing EPPE roles, click on **<Select Action>**.
5. Click on **<Add Role>** within the available Actions box on the EPPE application line.
6. Select the **<EPPE MicroStrategy User>** from the Select a Role dropdown menu.
7. Click on **<Next>**.
8. Enter any notes to the Approver in the **<Enter a Reason for Request>** filed.
9. Click **<Submit>**.
10. The **<Confirmation>** popup window displays.
11. Select **<OK>** to submit your request or **<Cancel>** to cancel your role request.
12. IDM provides you with a tracking number and emails you when the request has been processed.
13. Click on **<OK>**.

Back to Top

MSR002 - When a user has multiple roles within EPPE, how does MicroStrategy know for what role you are requesting reports?

MicroStrategy is aware of the roles that are assigned to a user within EPPE, and those roles are displayed and selectable by the user within MicroStrategy.

Back to Top

MSR003 - In MicroStrategy, can the fields/columns on the report result screen be expanded?

In MicroStrategy, the field/column width can be adjusted by placing the cursor in between two columns. The cursor will change to arrows pointing to the left and right. Click and drag to the desired width.

Back to Top

MSR004 - In MicroStrategy, can filters be applied to the report result screen?

Yes, MicroStrategy allows for filters to be applied on the report result screen. Right mouse click on any column heading and select **<Edit View Filter…>**. Follow the instructions on the screen.

Back to Top

Browsers (BRO)

BRO001 - Which browsers are supported by the CMS Enterprise Portal?

The CMS Enterprise Portal supports the following browsers:

1. Internet Explorer
2. Mozilla Firefox
3. Google Chrome
4. Safari
5. Microsoft Edge

Back to Top

BRO002 - What browser mode is supported?

There are different browser modes that can be specified by you, the user. Only the native browser mode is supported. For example, if you are using Internet Explorer 11, the supported browser mode is IE11. To find out what browser mode you are using, hit the F12 key while in IE. The top of the resulting window/panel will show the browser mode being used.

Back to Top

BRO003 - What document mode is supported?

There are different document modes that can be specified by you, the user. Only the native document mode is supported. For example, if the user is using Internet Explorer 8, the supported document mode is IE8 standards. If the user is using IE9, the supported document mode is IE9. To find out what document mode is being used, hit the F12 key while in IE. The top of the resulting window/panel will show the document mode being used.

Back to Top

BRO004 - Is JavaScript required for the CMS Enterprise Portal?

JavaScript needs to be enabled for successful use of the Enterprise Portal.

Back to Top

BRO005 - How do I clear my browser's cache using Internet Explorer (IE) 9, 10, and 11?

Sometimes it is necessary to clear your browser's cache. The cache is nothing more than a place on your hard disk where the browser keeps things that it downloaded in case they are needed again. To clear your Internet Explorer (IE) cache:

- Select Tools on the menu bar, then select Delete browsing history (or select Tools via the Gear Icon, then Safety and Delete browsing history).

- Make sure to uncheck Preserve Favorites Web site data and check both Temporary Internet Files and Cookies then click okay.
- You will receive a confirmation at the bottom of the window once it has successfully cleared your cache and cookies.

Back to Top

BRO006 - How do I clear my browser's cache using Google Chrome?

Sometimes it is necessary to clear your browser's cache. The cache is nothing more than a place on your hard disk where the browser keeps things that it downloaded in case they are needed again. To clear your cache using Google Chrome:

- While in Google Chrome hit Ctrl+Shift+Del.
- In the Clear browsing data window select "Beginning of Time" to delete everything.
- Be sure to select "Cookies and other site and plug in data" as well as "Cached images and files."
- Click on "Clear browsing data."

Back to Top

BRO007 - How do I clear my browser's cache using Mozilla Firefox?

Sometimes it is necessary to clear your browsers cache. The cache is nothing more than a place on your hard disk where the browser keeps things that it downloaded in case they are needed again. To clear your cache using Mozilla Firefox:

- While in Mozilla Firefox hit Ctrl+Shift+Del.
- In the Clear Recent History window, select "Everything" for Time range to clear.
- Click the drop down by Details and check the boxes for Cookies and Cache.
- Click on "Clear Now".

Back to Top

BRO008 - How do I clear my browser's cache using Microsoft Edge?

Sometimes it is necessary to clear your browsers cache. The cache is nothing more than a place on your hard disk where the browser keeps things that it downloaded in case they are needed again. To clear your cache using Microsoft Edge:

- While in Microsoft Edge hit Ctrl+Shift+Del.
- Under the dropdown for the "Time Range", select "All time".
- In the Clear Browsing data window, select "Cookies and other site data" and "Cached images and files".
- Click on "Clear Now".

Back to Top

BRO009 - How do I enable pop-ups in Internet Explorer?

Sometimes it is necessary to allow certain pop-ups from an application. To allow pop-ups in Internet Explorer, follow the below steps:

- Select Tools on the menu bar (or select Tools via the Gear Icon.
- Click on “Internet Options.”
- Click on the “Privacy” tab.
- Click on “Settings” in the Pop-up Blocker section.
- Add https://portal.cms.gov to the “Address of website to allow” field.
- Click on “Add.”
- Click on “Close.”
- Click on “OK.”

Back to Top

BRO010 - How do I enable pop-ups in Google Chrome?

Sometimes it is necessary to allow certain pop-ups from an application. To allow pop-ups in Google Chrome, follow the below steps:

- Click on customize Google Chrome button (icon with three horizontal black lines).
- Click on “Settings.”
- On the very bottom of that screen, click on “Show advanced settings.”
- Under the “Privacy” title click on “Content settings.”
- Scroll to the “Pop-ups” section and click on “Manage exceptions.”
- In the “Hostname pattern” field type https://portal.cms.gov.
- Ensure that “Allow” is selected in the “Behavior” field.
- Click on “Done.”
- Click on “Done.”
- Close the “Settings” tab.

Back to Top

BRO011 - How do I enable pop-ups in Mozilla Firefox?

Sometimes it is necessary to allow certain pop-ups from an application. To allow pop-ups in Mozilla Firefox, follow the below steps:

- Click on customize Firefox button (icon with three horizontal black lines).
- Click on “Options.”
- On the left-hand side click on “Content.”
- Under the “Pop-ups” section click on “Exceptions.”
- Type https://portal.cms.gov in the “Address of website” field.
- Click on “Allow”.
- Click on “Save Changes.”
- Close the “Options” tab.

Back to Top

BRO012 - How do I enable pop-ups in Microsoft Edge?

Sometimes it is necessary to allow certain pop-ups from an application. To allow pop-ups in Microsoft Edge, follow the below steps:

- Click on the ellipsis icon to customize Microsoft Edge (icon with three horizontal black dots).
- Click on “Settings.”
- On the left side of that screen, click on “Cookies and site permissions”.
- Under the Cookies and site permission page click on “Pop-ups and redirects”.
- Under the “Allow” section, click on “Add”.
- The “Add a site” pop-up window appears. In the “Site” field type https://portal.cms.gov.
- Click on “Add.”
- Close the “Settings” tab.

Back to Top

Errors (ERR)

ERR001 - What do I do when I receive a “This Portlet is Unavailable” error?

When receiving the Portlet is Unavailable error, use the back button followed by the refresh button, and attempt your action again. If the error persists, clear your browser’s cache and cookies, log out and in again, and attempt your action again. If you still receive the error, please take a screenshot including the clock on the bottom right-hand side of your screen and send it to the EPPE Help Desk. Please include detailed information as to what you were doing when the error was received.

Back to Top

ERR002 - What do I do when I receive a “Request Failed” error?

When receiving the Request Failed error, use the back button followed by the refresh button, and attempt your action again. If the error persists, clear your browser’s cache and cookies, log out and in again, and attempt your action again. If you still receive the error, please take a screenshot including the clock on the bottom right-hand side and send it to the EPPE Help Desk with detailed information as to what you were doing when the error was received.

Back to Top