EIDM Instructions for MACPro Users

Version: 3.0

Date: 12/18/17

Table of Contents

Welcome to the EIDM Instructions for MACPro Users

The EIDM Instructions for MACPro Users describes steps MACPro users should take to obtain EIDM IDs and request access to MACPro. Please contact the Help Desk if you have questions outside the scope of this document.

Assistance with MACPro is available through the MACPro Help Desk, Monday through Friday, 9:00 am-7:00 pm Eastern Standard Time. For questions regarding the *use of MACPro*, contact the MACPro Help Desk via email at MACPro_HelpDesk@cms.hhs.gov or call 301-547-4688.

The MACPro Help Desk Team welcomes your suggestions for our training and reference materials. Please contact us with your feedback and comments on this training, or if you need other MACPro assistance.

Table 1: Key Terms

Select each term for further information.

Table 1: Key Terms

Term	Abbreviation/Description
EIDM Portal	CMS Enterprise Identity Management Portal
CMS Secure Portal	The link to login to the EIDM Portal
RIDP	Remote Identity Proofing
MFA	Multi-Factor Authentication
EIDM ID	An EIDM ID provides access to EIDM through the CMS Enterprise Portal. Having an EIDM ID does not mean a user has access to MACPro. After registering an EIDM ID, a user must request access to MACPro, select an EIDM role for MACPro, and receive approval.
MACPro Role	The MACPro Role you will hold within MACPro. This is separate from the roles you request within EIDM. In MACPro there are roles that allow you perform different functions within the system.
EIDM Role for MACPro	The MACPro Role you will hold in EIDM. This is separate from roles requested within MACPro. In EIDM there are general roles that correspond with the roles in MACPro. For example, a user should request the EIDM role of MACPro State User if the user holds the MACPro role of State Editor.

What is EIDM?

The CMS Enterprise Identity Management (EIDM) Portal is an identity management and services system that provides users with access to Centers for Medicare and Medicaid Services (CMS) applications. An EIDM account ensures that only authorized and registered users can access protected information and systems through the CMS Enterprise Portal. This system replaces the previous Individuals Authorized Access to CMS Computer Services (IACS) system, for which users requested access in 2013.

What is MACPro?

MACPro is a web-based application for the submission, review, disposition, and management support of Medicaid and CHIP initiatives, Quality Measures Reporting, State Plan Amendments (SPA), Waivers, Demonstrations and Advance Planning Documents. MACPro replaces CARTS for Adult and Child Core Set reporting and is the new application for Health Homes Core Set reporting.

MACPro is being implemented to improve the state reporting and federal review processes, federal program management, and transparency. It also supports data-driven decision making for Medicaid and CHIP programs through online access to data and information. MACPro will be one of the many different CMS applications integrated within EIDM.

MACPro integration into EIDM

The Medicaid and CHIP Program System (MACPro), https://macpro.cms.gov, is connected to the CMS Enterprise Identity Management (EIDM) Portal, https://portal.cms.gov . Users access MACPro through EIDM. All existing and potential MACPro users, regardless of user role, are required to have an EIDM ID.

- Once you have an EIDM ID, or if you have previously obtained one, you will need to request MACPro access through EIDM and select an EIDM role for MACPro.

- **Unless notified otherwise, all State users should request the State User role and all CMS users should request the CMS Staff User role in EIDM.**

- When requesting access, you may be subject to Remote Identity Proofing, a process within EIDM that verifies your identity. Your EIDM role request for MACPro will go through the approval process to CMS. When your role request is approved, you will be granted access to the MACPro application to begin or continue working in MACPro.

Figure 1: EIDM MACPro Integration Workflow

The image below displays the steps needed to register for an EIDM ID and to request access to MACPro through EIDM.
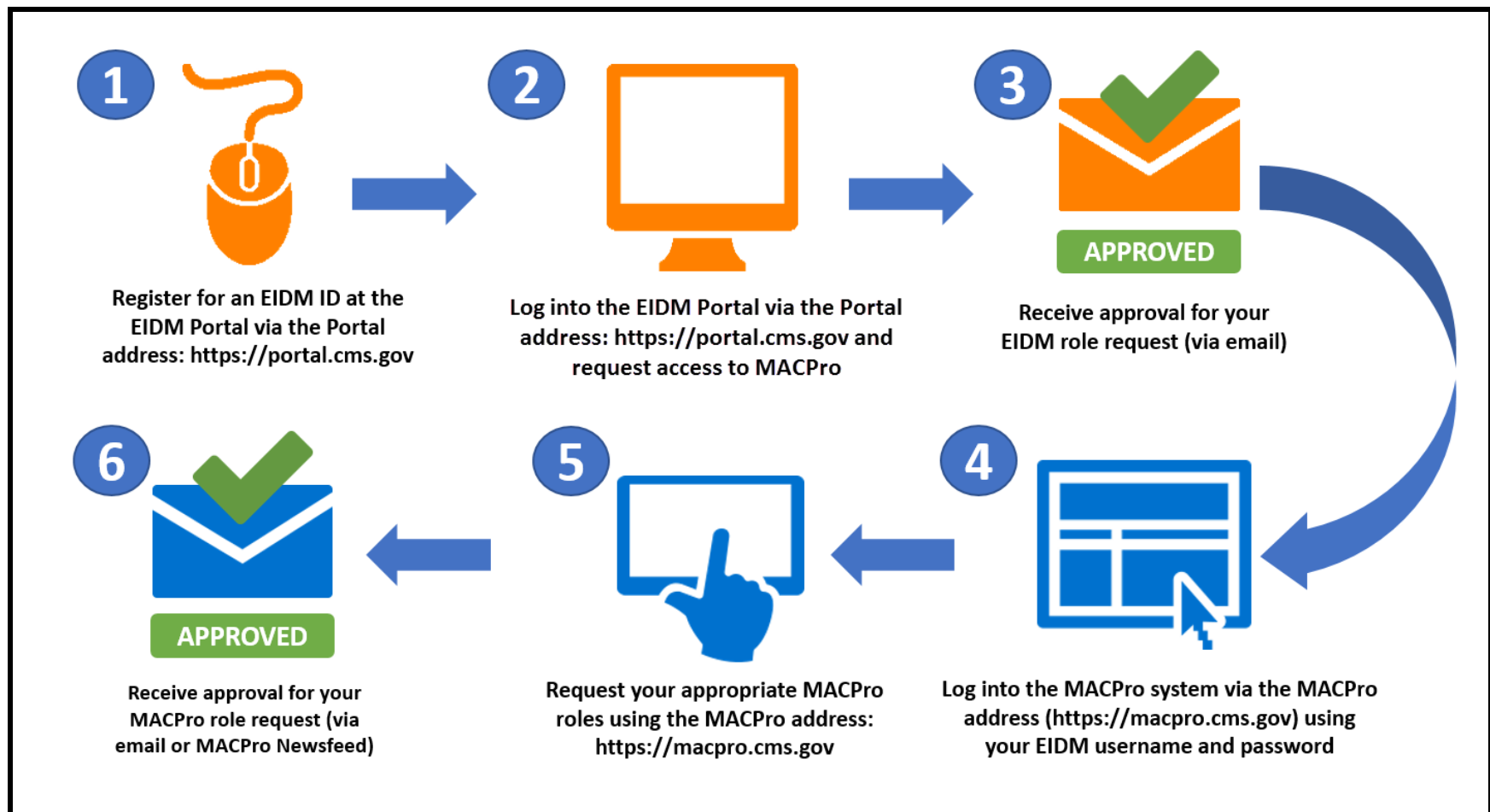

Figure 1: EIDM MACPro Integration Workflow

Table 2: EIDM User Role Table

The table below displays the MACPro roles available in EIDM with corresponding descriptions. This table may be used to determine your role when requesting MACPro access in EIDM.

Table 2: EIDM User Role Table

EIDM Roles	Description
MACPro State User	U.S. State and Territories users This role will grant users access to MACPro application's state workflow and application's state reports **All State users should select this role unless notified otherwise.**
MACPro CMS Staff User	CMS Central and Regional Office Staff users This role will grant users access to MACPro application's CMS workflow and application's non-management reports **All CMS users should select this role unless notified otherwise.**
MACPro Business Support User	Non-CMS MACPro users. This role is for CMS Contractors who need access to MACPro application.
MACPro Approver	CMS Central and Regional Office Staff users. This role is responsible for approving EIDM roles requested for CMS Central and Regional Office users. This approver role does not approve role requests within the MACPro application. **Note**: There will be at least one of these roles for CMS Central Office and at least one for each of the 10 CMS Regional Offices. The end user role requests are routed to these approvers by Central Office and Regional Offices.
MACPro Help Desk	CMS MACPro Helpdesk users This role is responsible for regular Helpdesk activities like Reset Password, Unlock Account, etc.
MACPro Business Owner	This is a restricted role, for CMS users who are responsible for approving MACPro Helpdesk and MACPro Approver role requests. This will not be available in the drop-down box for the general user population.

Figure 2: EIDM Role Approval Hierarchy

The image below displays the role approval hierarchy for MACPro roles within EIDM. Each tier approves the tier below it.
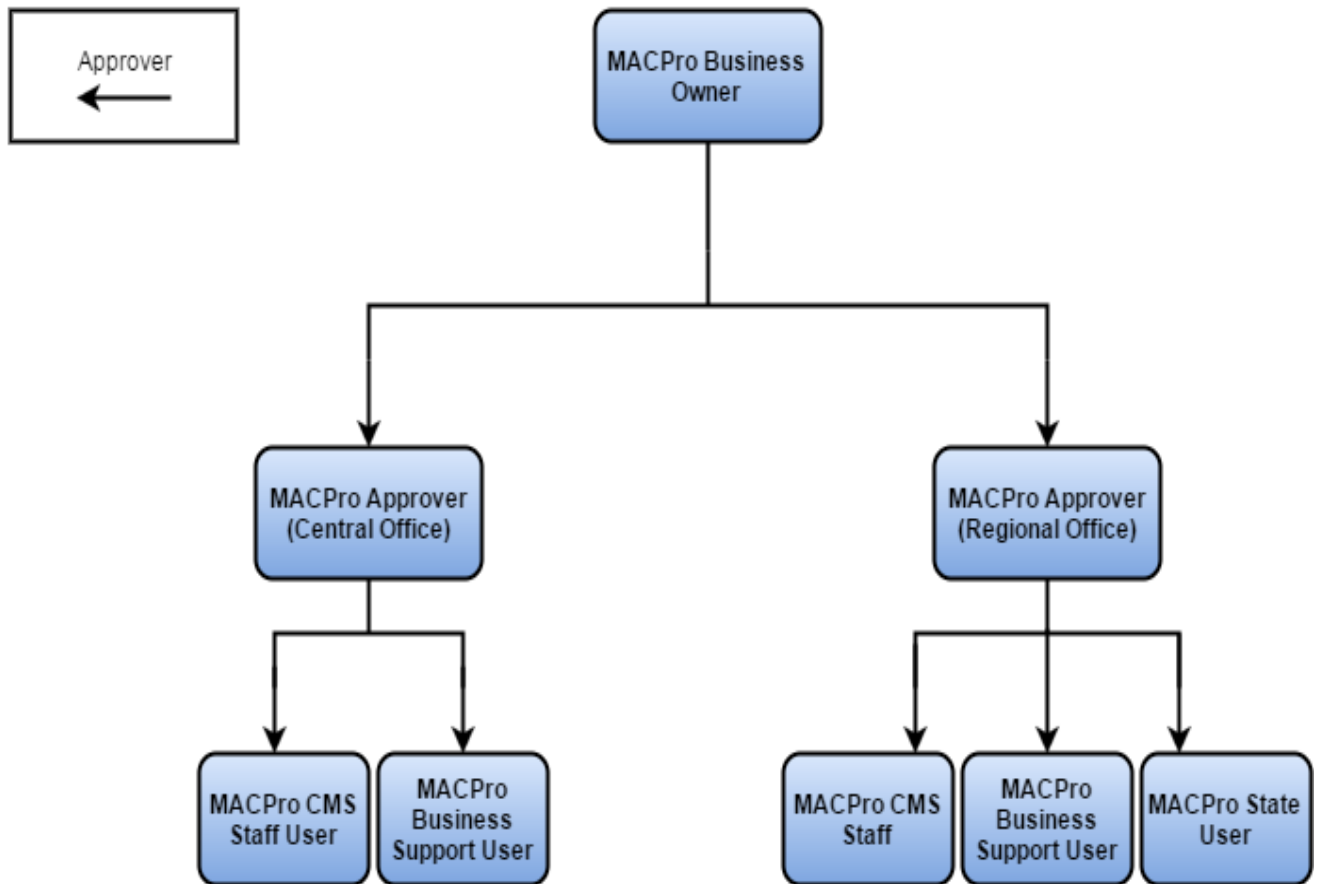
Figure 2: EIDM Role Approval Hierarchy

Scenarios

Select the following scenario that applies to you to continue obtaining an EIDM ID or requesting an EIDM role for MACPro:

1. **Do you already have an EIDM ID?**
   a. Begin with assuring that your challenge questions, password and personal information are up to date. Once completed, proceed to request an EIDM MACPro role.

2. **Are you a new user? (You do not have an EIDM ID)**
   a. Begin with registering for an EIDM ID.

3. **Are you not sure?**
   a. Begin with selecting the Forgot User ID link. Once your information is verified and you have received your User ID, select the Forgot Password link. If you do not know your challenge questions, please contact the MACPro Help Desk at MACPro_HelpDesk@cms.hhs.gov. If your information can't be verified, then proceed to follow the instructions for New User Registration.

Step 1: Register for an EIDM ID

All MACPro users must first register as a user through the Centers for Medicare and Medicaid (CMS) Enterprise Identify Management (EIDM) Portal. To create your EIDM profile, provide necessary information and set up your User ID, password, and your challenge questions.

1. Go to the Enterprise Portal at https://portal.cms.gov. (You can use Internet Explorer 11, Firefox, or Chrome)

2. Select "**New User Registration**" on the home page.
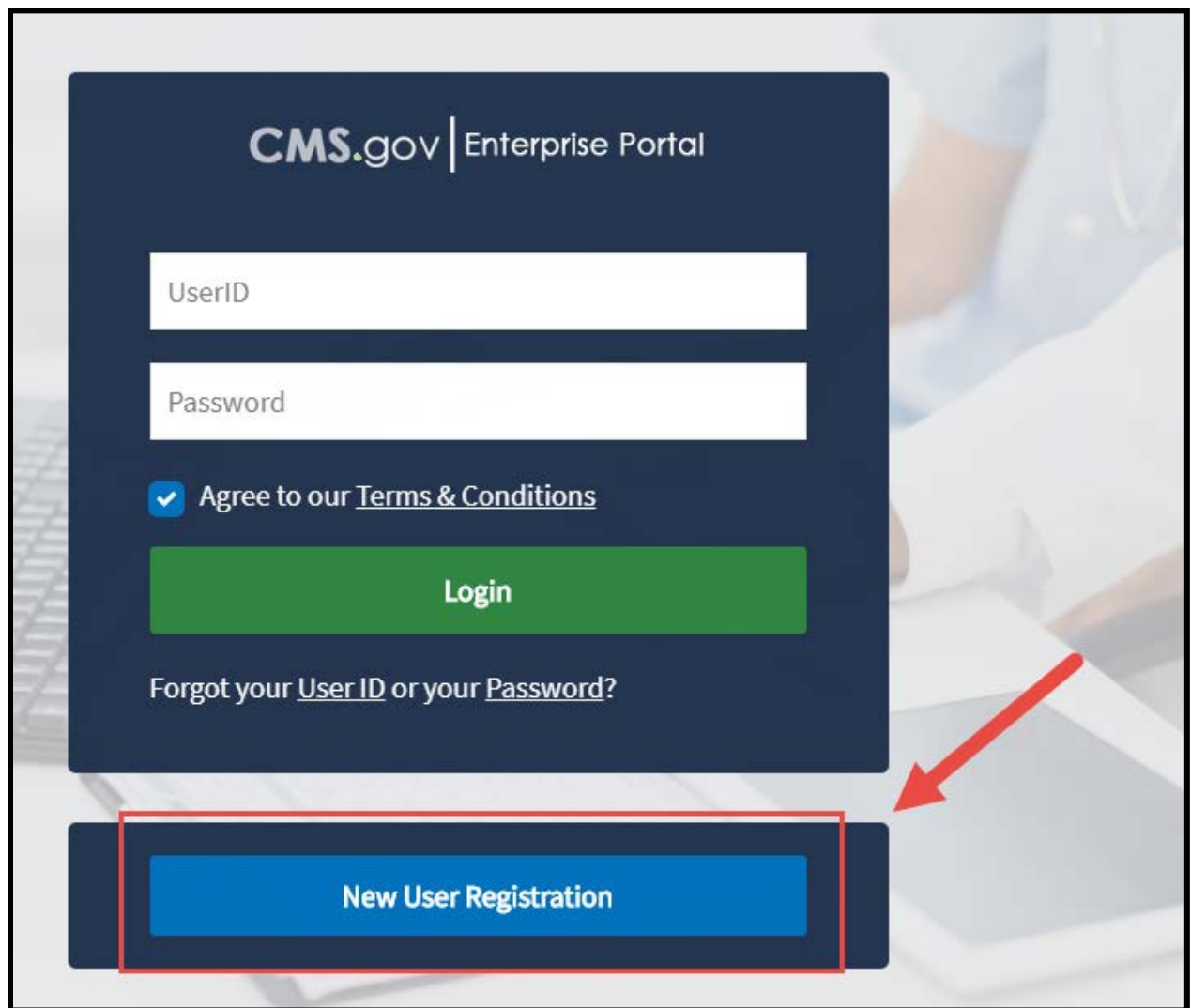
Figure 3: New User Registration button

3. Select your application from the drop-down list.
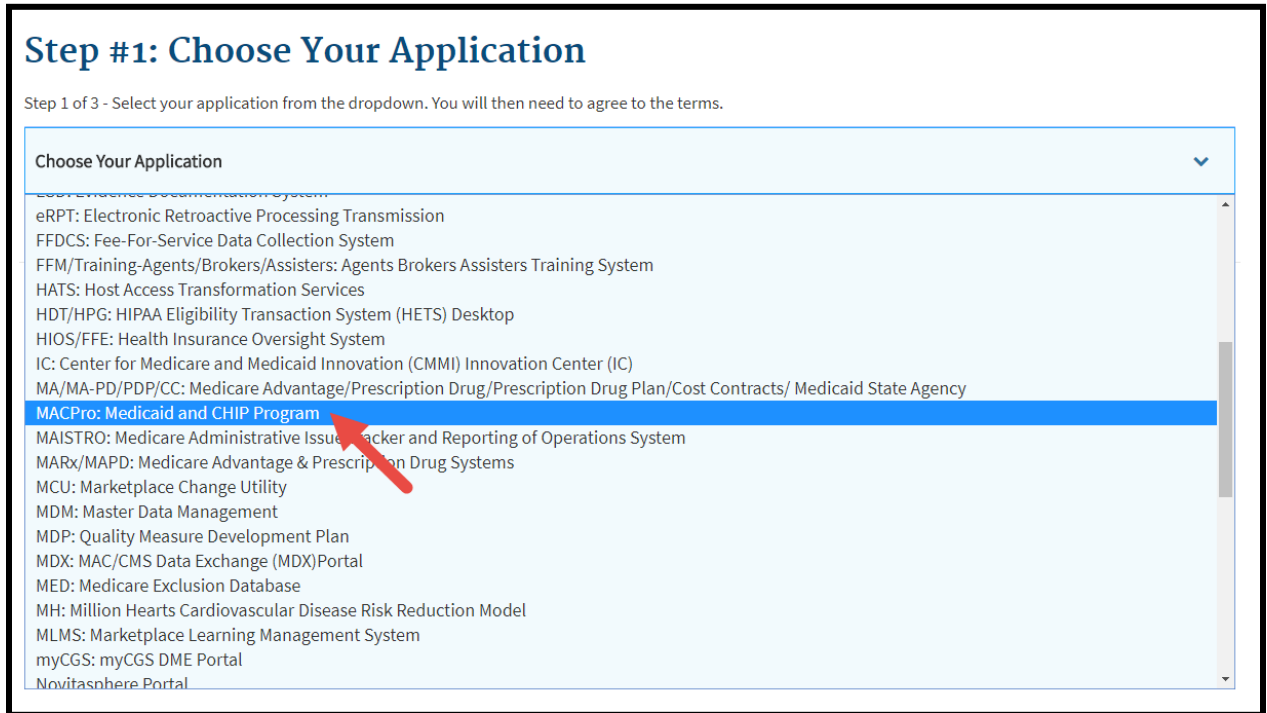
Figure 4: MACPro: Medicaid and CHIP Program option in drop-down list

4. Accept the **Terms and Conditions** by checking the box at the bottom of the page. Then, select "**Next**" to continue.
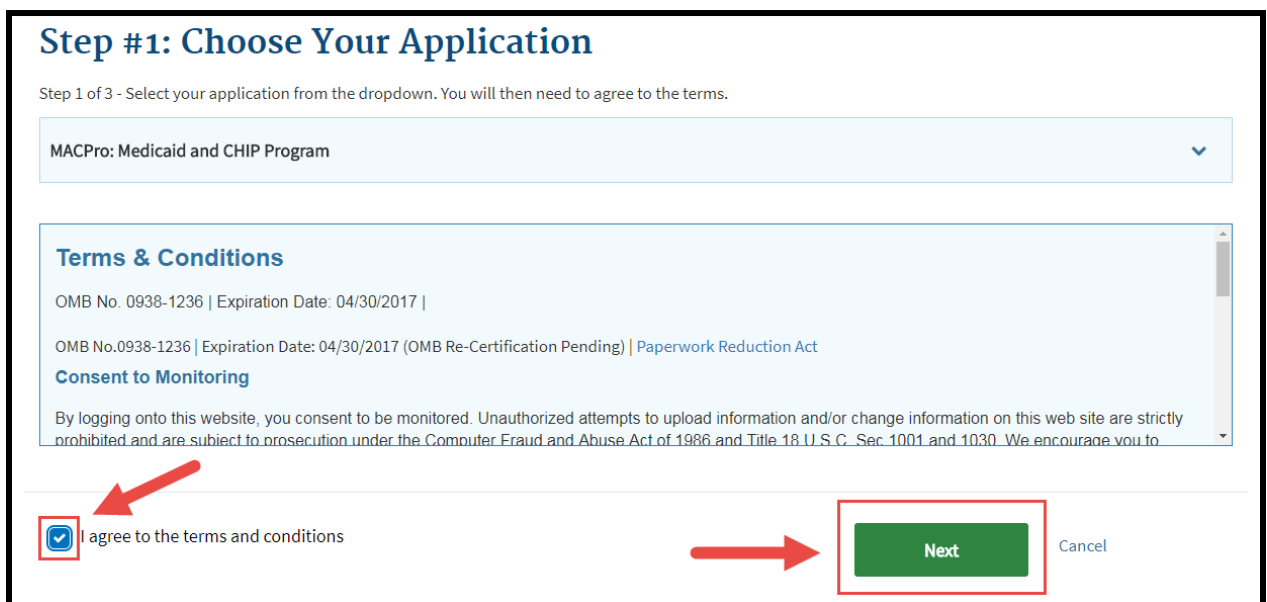
Figure 5: Terms and Conditions acceptance checkbox and Next button

5. Enter in your information as required. Please note that all fields are required fields except for the field asking for your Social Security Number. When complete, select "**Next**" at the bottom of the page.

Figure 6: Register Your Information page and Next button

6. Create your EIDM User ID, Password and Challenge Questions. Once complete, select "**Next**".

Figure 7: Create User ID, Password and Security page and Next button

Please Note:

- Your **User ID** must follow these requirements:
    - It must be a minimum of 6 and maximum 74 alphanumeric characters
    - It must contain at least 1 letter
    - It may **not** contain your Social Security Number or any 9 consecutive number
    - The only special characters that are allowed are dashed (-), underscored (_), apostrophes ('), @ and periods (.) followed by alphanumeric characters
- Your **password** must follow these requirements:
    - It must be changed every 60 days
    - It must be a minimum of 8 and a maximum of 20 characters
    - It can be changed only once every 24 hours
    - It must contain at least 1 letter and 1 number
    - It must contain at least 1 upper case and 1 lower case letter
    - It must contain at least 1 special character
    - It must be different than previous passwords used
    - It may **not** contain the User ID
    - It may **not** contain commonly used words
    - The following special characters may **not** be used ? < > ( ) ' " / \ &.

7. You will then be directed to a Registration Summary page, please review all information entered to ensure it is correct and confirm your e-mail address as necessary.

Figure 8: Registration Summary page and Confirm E-Mail Address field

8. On the same screen, also verify your user ID and challenge questions. Then select "**Submit User**".

Figure 9: Submit User button

9. A confirmation message will appear stating that an email will be sent to your email address.
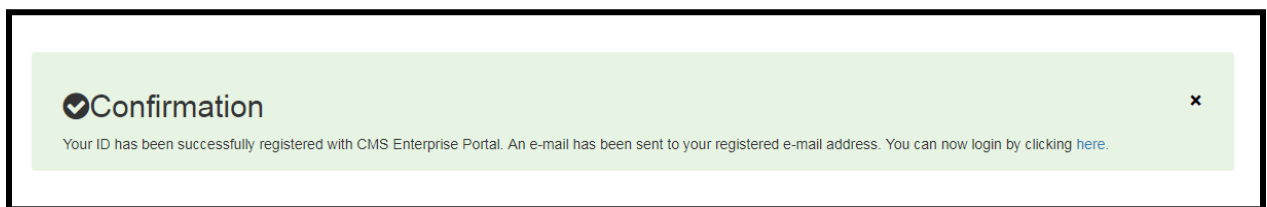
Figure 10: Confirmation message

10. The next steps you will take are for requesting an EIDM role for MACPro. Please follow the instructions in Step 2 for requesting a role.

Step 2: Request Access to MACPro

The next step is to request access to MACPro by requesting your **EIDM role for MACPro**. Once this is approved, you will be able to access MACPro.

Please Note: Your EIDM role for MACPro is different than your MACPro role. Your EIDM role for MACPro only provides access to MACPro. Your MACPro role will provide specific action permissions within the MACPro application. If you are a new user, you will need to request roles in MACPro to begin using MACPro.

1. Login to the CMS Enterprise Portal by entering your User ID and Password. Accept the Terms and Conditions by checking the box in front of "**Agree to our Terms and Conditions**". The Terms and Conditions can be accessed by clicking on the link labeled "**Terms and Conditions**"
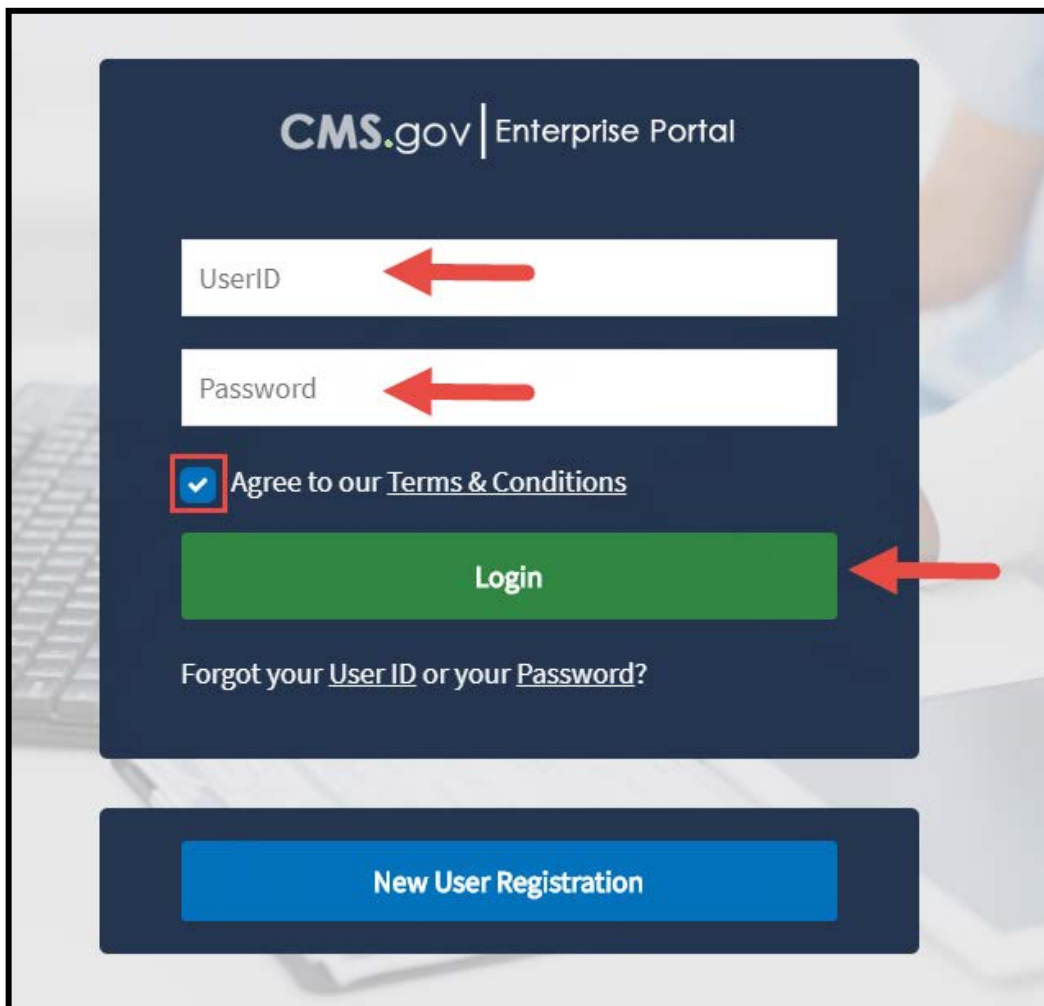
Figure 11: CMS Enterprise Portal log in screen

2. On the top banner, under your name, you can select "**My Access**" from the drop-down menu to request a role. Or you can also select "**Request/Add Apps"** on the "My Portal" page.
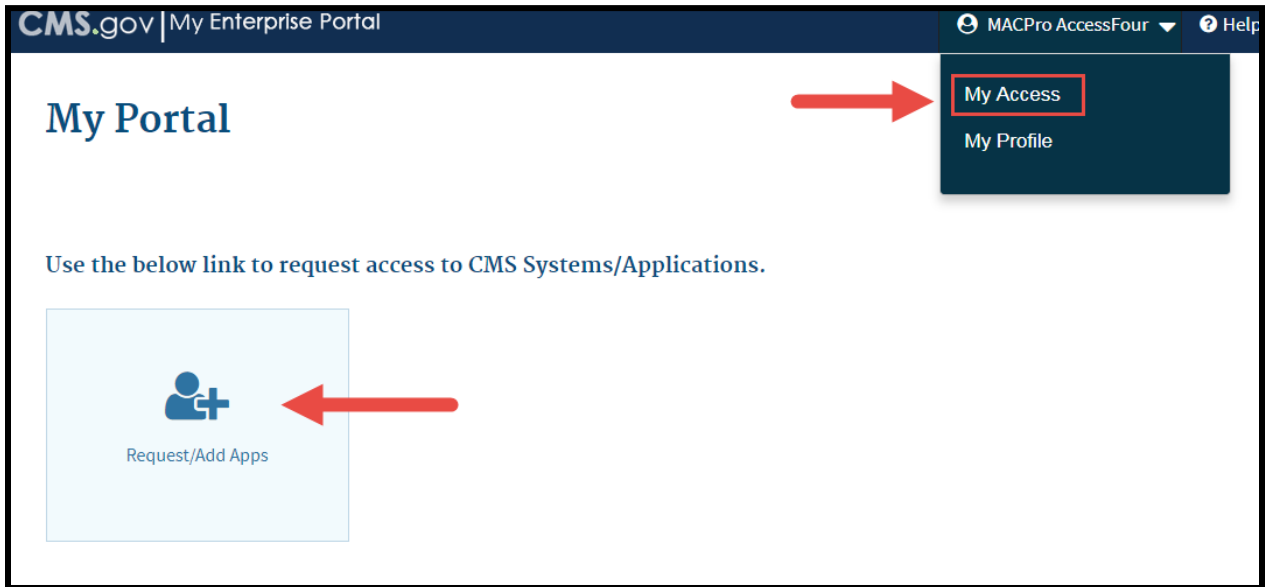
Figure 12: My Access option in drop-down menu and Request/Add Apps link

3. On the next screen, type the word "**MACPro**" in the Access Catalog filter bar.
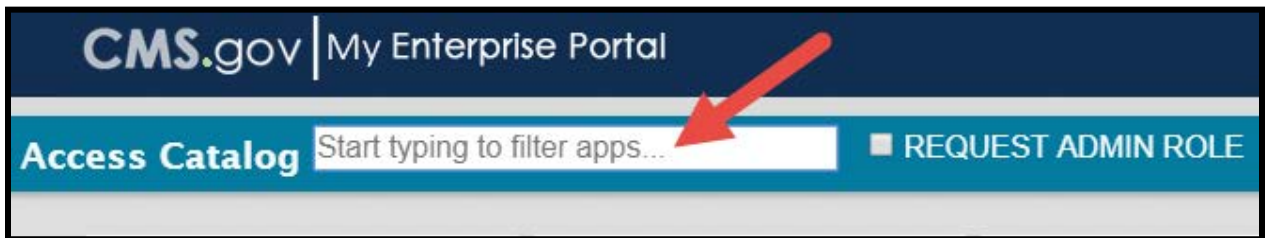
Figure 13: Access Catalog filter bar

4. When the MACPro tile appears, select the grey "**Request Access**" button in the tile.
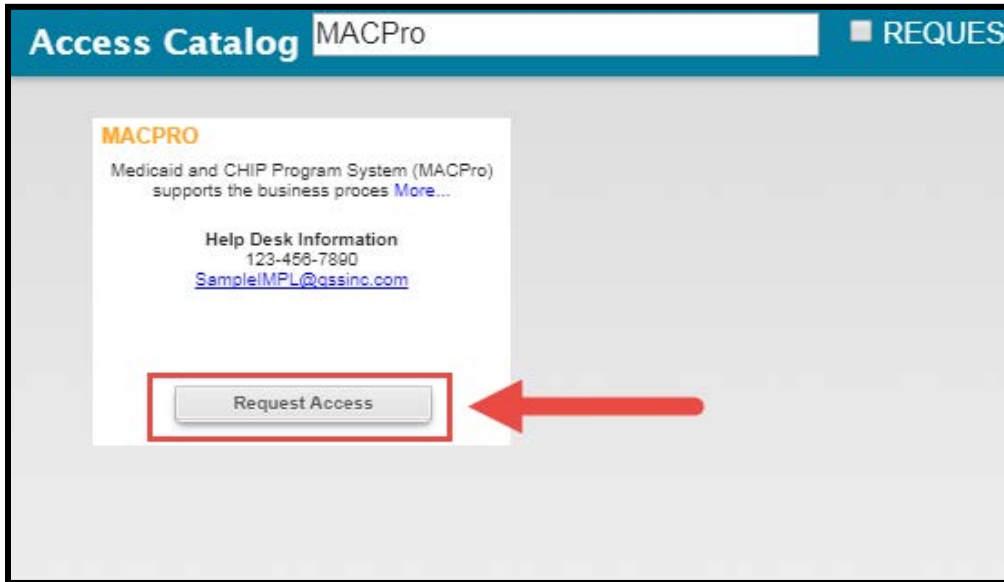
Figure 14: Request Access button

5. The System Description field will automatically populate with the MACPro option. In the Role drop-down, select the EIDM role that corresponds with your MACPro Role. For example, if you have a State role in MACPro you would select "MACPro State User". **(All State users should select the "State User" role and all CMS users should select the "CMS Staff User" role, unless notified otherwise).**
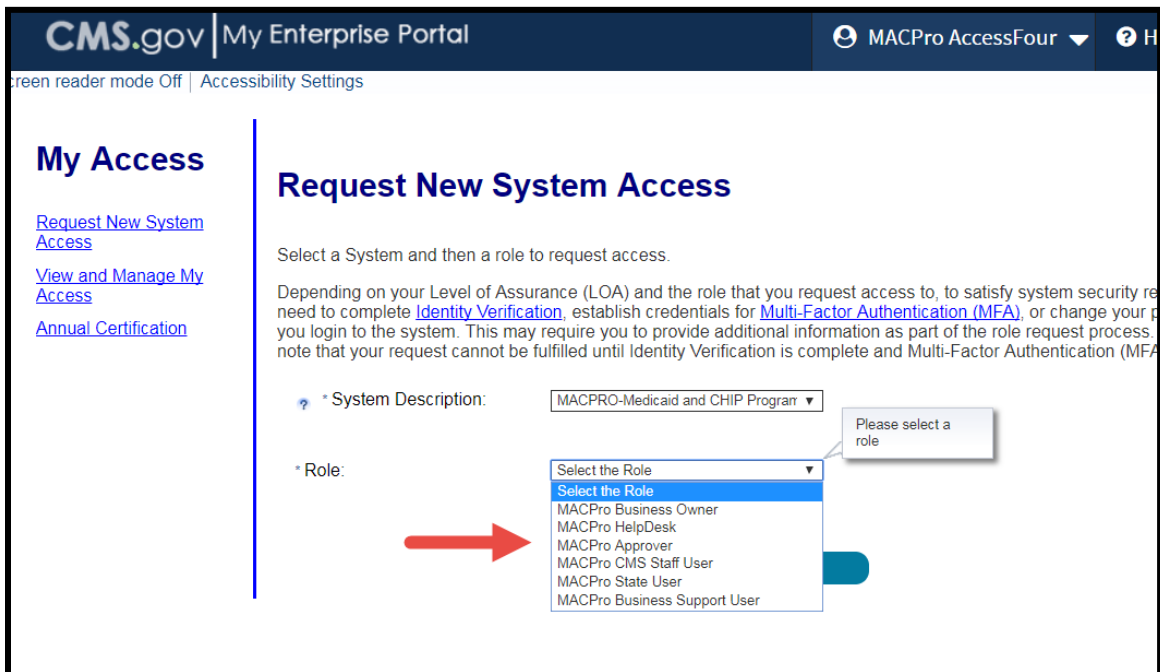
Figure 15: Request New System Access page

a) If you select a MACPro CMS Staff User Role or a Business Support User Role, choose a region:

Figure 16: CMS Region drop-down menu

b) If you select a MACPro State User Role, choose the region that your state belongs to and then choose your state:

Figure 17: Region drop-down menu and State and Territories drop-down menu

6. Next, enter in any notes to the approver and then select "**Submit**".

Figure 18: Submit button

7. After submitting your request, you may be directed to Identity Verification. If so, please continue to Step 3 for further instruction. **Please note: Unless previously completed, all users will be subject to pass through mandatory Identity Verification (Step 3) prior to receiving the optional MFA prompt.** All users will be asked if you would like to add Multi-Factor Authentication as shown in the screenshot below. While MFA is not required for MACPro users, you may want to add MFA to have an additional level of security to prevent unauthorized access to your account. If you choose to add MFA please select the "**Add MFA**" button and refer to Step 4 for further instruction. If you choose to bypass MFA please select the "**Skip MFA**" button.
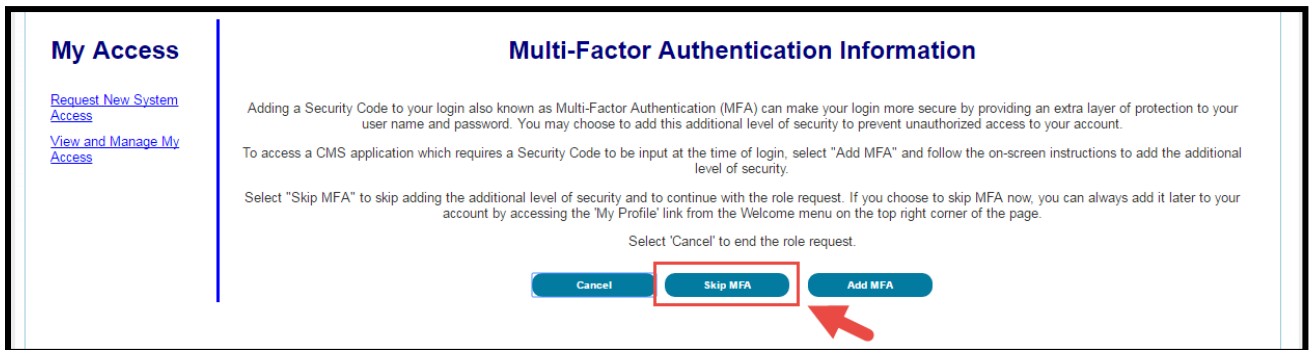
Figure 19: Skip MFA button

8. When Identity Verification is completed and/or MFA is skipped/added, you will be directed to the Request Acknowledgment screen. This screen indicates that you will also receive an email notification that you your role request has been processed. Select "**Ok**".
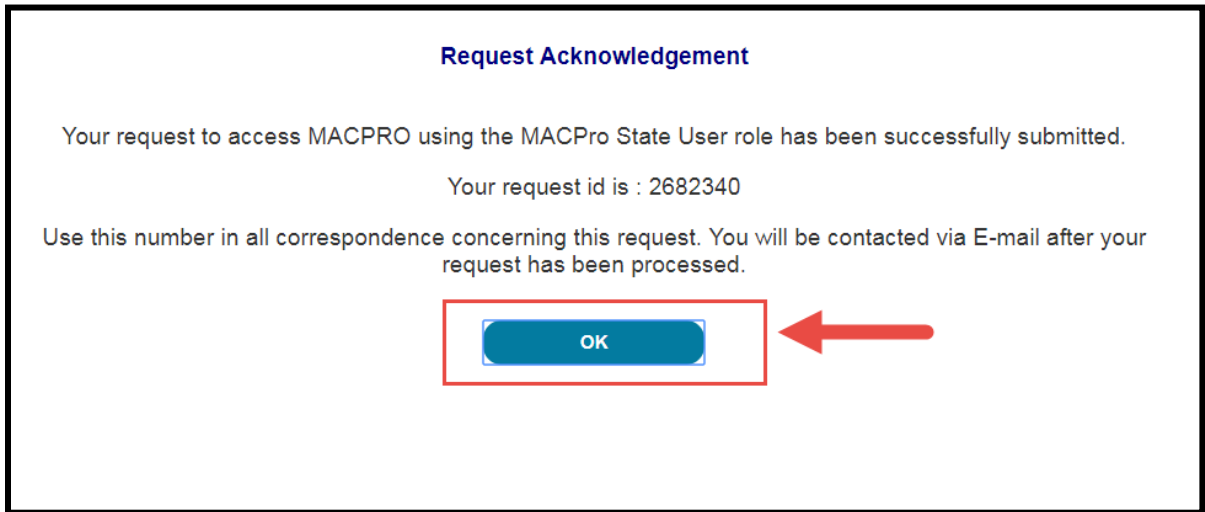
Figure 20: OK button

9. Once you have select "**Ok**" you will be directed to the View and Manage My Access Screen. In this table you will be able to see any roles that you currently hold, as well as any pending requests.
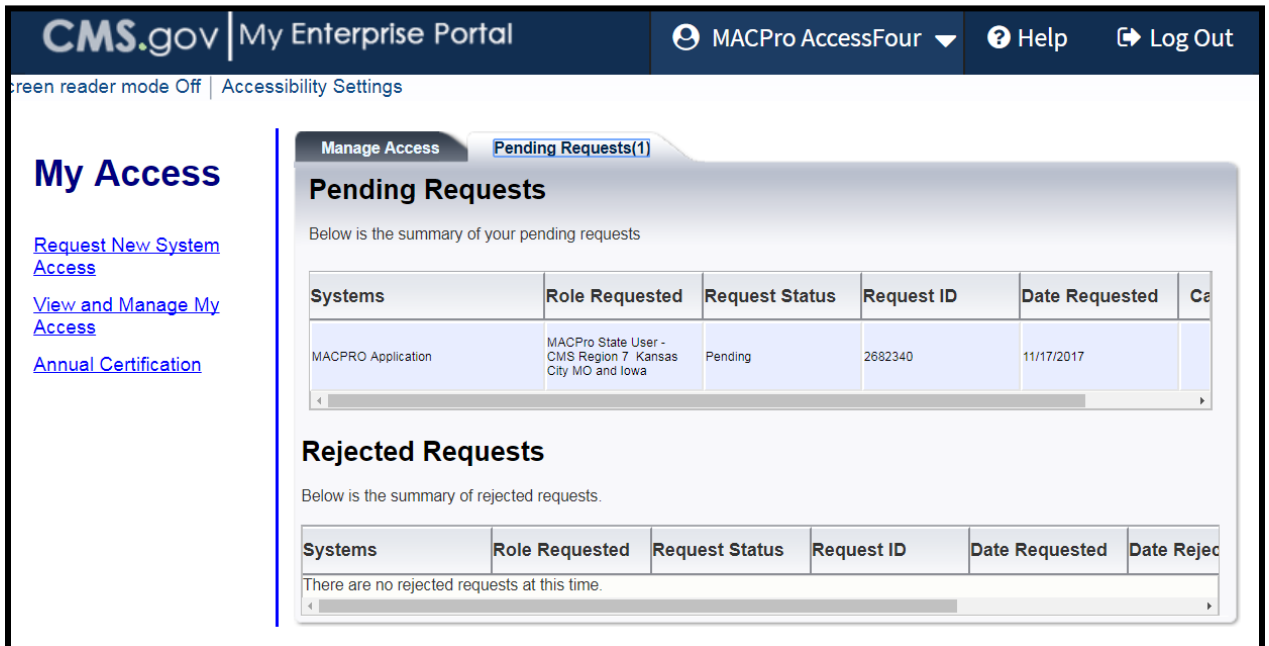

Figure 21: View and Manage My Access screen

10. When your role request has been approved or rejected you will receive an email notification indicating this information.

Step 3: Verify Identity Online with Remote Identity Proofing (RIDP)

What is Identity Verification?

Identity Verification is the process of providing sufficient information (e.g., identity history, credentials, or documents) to a service provider for proving that an individual is who he/she claims to be. Individuals requesting electronic access to CMS protected information or systems must be identity proofed prior to being given access.

The Identity Verification process is necessary for all EIDM Roles for MACPro.

When selecting a role for MACPro you may be redirected to RIDP. RIDP is typically completed via an online questionnaire. If you fail the RIDP questionnaire, please follow these steps:

1. **Take a screenshot of the notification message that indicates you were NOT able to be verified.**
2. Attempt the role request process again (refer to Step 2 in this document).
3. This time when prompted to repeat RIDP, ensure that you have entered your Personal Information correctly (i.e. your personal home address, your personal phone number, etc.).
4. After verifying your personal information complete RIDP.
5. If your information is correct and you are still unable to be verified, then call the Experian Verification Support Service number that is displayed in the message indicating you cannot be verified. Please note: Experian will attempt to verify your identity by asking further Out-of-Wallet questions.
6. If Experian is not able to verify you as a person, then send the screenshot of the notification that indicates you are unable to be verified to the MACPro_HelpDesk@cms.hhs.gov along with your EIDM ID.

Completing RIDP

1. Once you select a MACPro role in EIDM, you may be taken to the Identity Verification Page. Select "**Next**".
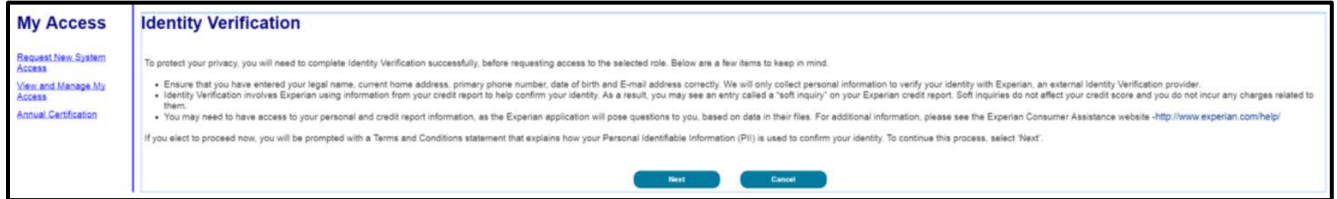
Figure 22: Identity Verification Page

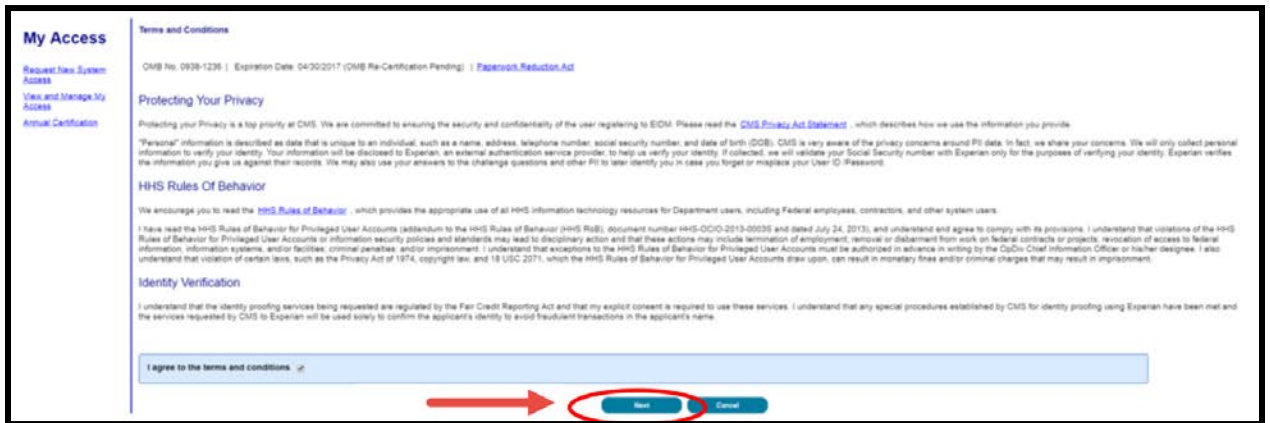2. Agree to the terms and conditions by checking the box. Then select "**Next**".

Figure 23: Next button

3. You will have the opportunity to verify your personal information. Once verified, select "**Next**".

Figure 24: Your Information page and Next button

4. Depending on your provided personal information, the Verify Identity page might show up. You will be required to answer several Out-of-Wallet (OOW) questions about information that may be in your personal records. Please choose your answers carefully. Select the "**Next"** button when you are ready to submit.

Figure 25: Verify Identity Page and Next button

5. Once you have submitted, you should receive a confirmation notice. Select "**Next**".
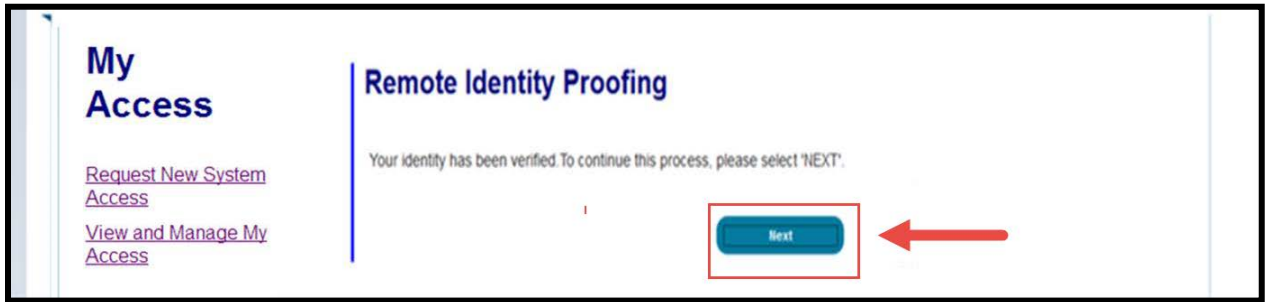
Figure 26: Remote Identity Proofing confirmation notice

6. A Request Acknowledgement message should appear. Select "**Ok**".
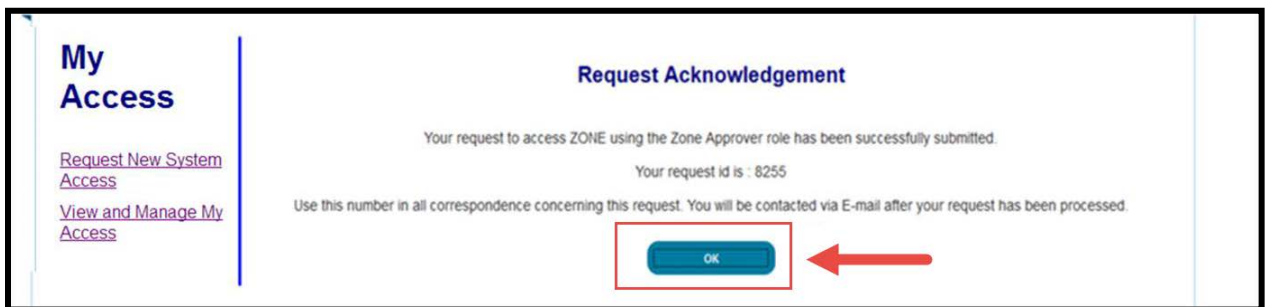
Figure 27: Request Acknowledgement message

7. If you cannot be verified as a person you will receive a message that indicates you have not passed. First, **take a screen shot of the message as shown below**. Then repeat the role request process detailed in Step 2 of this document. When prompted to repeat RIDP, ensure that you have entered your personal information correctly (i.e. your personal home address, your personal phone number, etc.). Then continue to complete RIDP. If your information is correct and you are still unable to pass, then call the Experian Verification Support Service number that is displayed in the message. If you cannot be verified after contacting Experian, please send a screenshot of the notification to MACPro_Helpdesk@cms.hhs.gov along with your EIDM ID.
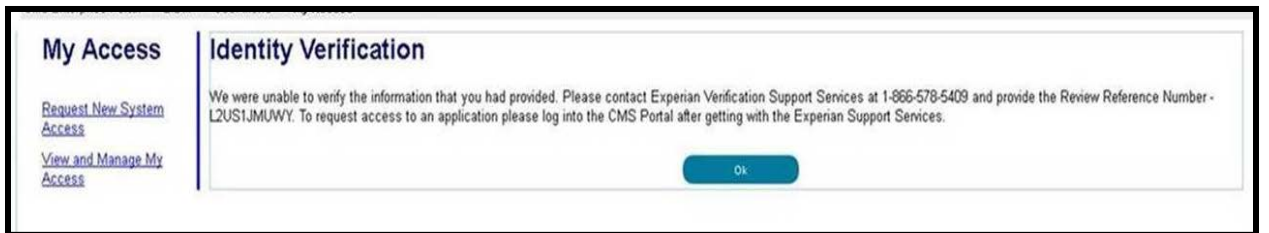
Figure 28: Identity Verification not passed message

Step 4: Multi-Factor Authentication (MFA)

What is Multi-Factor Authentication (MFA)?

MFA is a type of login (authentication) that, in addition to a user ID and password, requires another "factor" such as a Security Code. To comply with CMS policy, most users will need to establish a second login "factor" commensurate with the level of access requested. CMS uses Symantec's Validation and Identity Protection (VIP) service to add a second layer of protection for your online identity. Symantec provides validation and identity protection through computer, phone, and E-mail.

If a user selects to add MFA, the CMS EIDM Portal requires registration of a phone or computer to add an additional level of security to a user's account. The user is given four options to select from to complete the registration process.

Please note: that MFA is optional for MACPro Roles in EIDM.

MFA Registration

1. Log into the CMS Enterprise Portal by entering your User ID and Password. Accept the Terms and Conditions by checking the box in front of "**Agree to our Terms and Conditions**". The Terms and Conditions can be accessed by clicking on the link labeled "**Terms and Conditions**"

Figure 29: CMS Enterprise Portal log in screen

2. In the top banner select "My Profile" under your name.
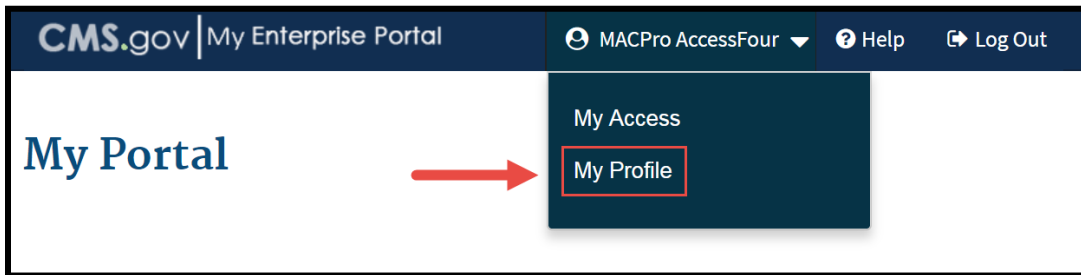
Figure 30: My Profile link

3. Select "**Register MFA**" from the left panel.

Figure 31: Register MFA link

4. Choose the device that you wish to register you MFA with from the dropdown list. Please note the following:

MFA Device Information:

- For Tablets/Computers/Laptops enter the Credential ID generated by the VIP Access client.

- For Text and Interactive Voice Response (IVR) options, you will be asked to enter a valid phone number to receive your Security Code.

- For the E-mail option, the E-mail address from your profile will automatically be used to send a Security Code.
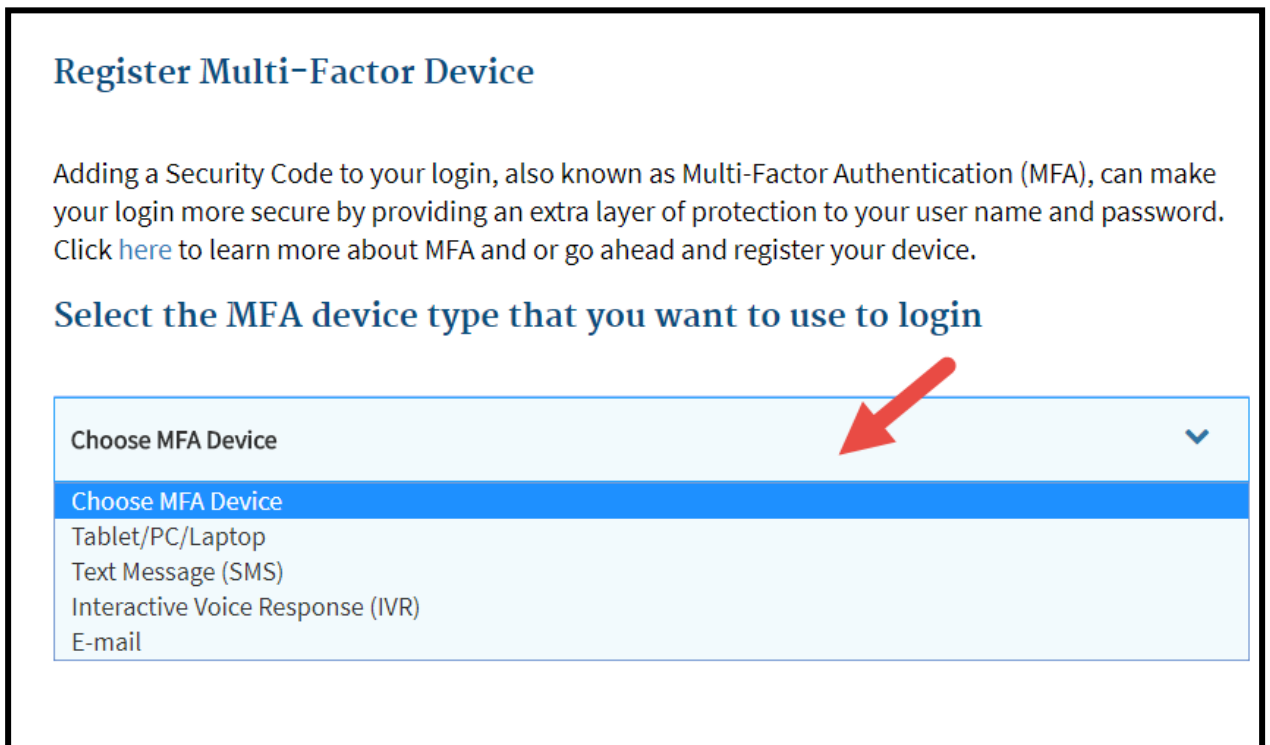
Figure 32: Choose MFA Device drop-down menu

5. Depending on the device you select, you may have to enter further information. Once entered, select "**Submit**".

Register Multi-Factor Device

Adding a Security Code to your login, also known as Multi-Factor Authentication (MFA), can make your login more secure by providing an extra layer of protection to your user name and password. Click here to learn more about MFA and or go ahead and register your device.

Select the MFA device type that you want to use to login

E-mail

The E-mail address on your profile will automatically be used for the E-mail option. Your e-mail address cannot be changed at the time of MFA registration. To change your E-mail, please select 'Change E-Mail Address' from the 'Change My Profile' menu.

macpro_helpdesk@cms.hhs.gov

Enter MFA Device Description

Submit   Cancel

Figure 33: Enter MFA Device Description field and Submit button

6. Once you have registered a device, you will receive a confirmation message.

MFA Login

1. Log into the CMS Enterprise Portal by entering your User ID and Password.

Figure 34: CMS Enterprise Portal log in screen

2. Next select an MFA device from the drop-down menu labeled "**Choose MFA Device**".
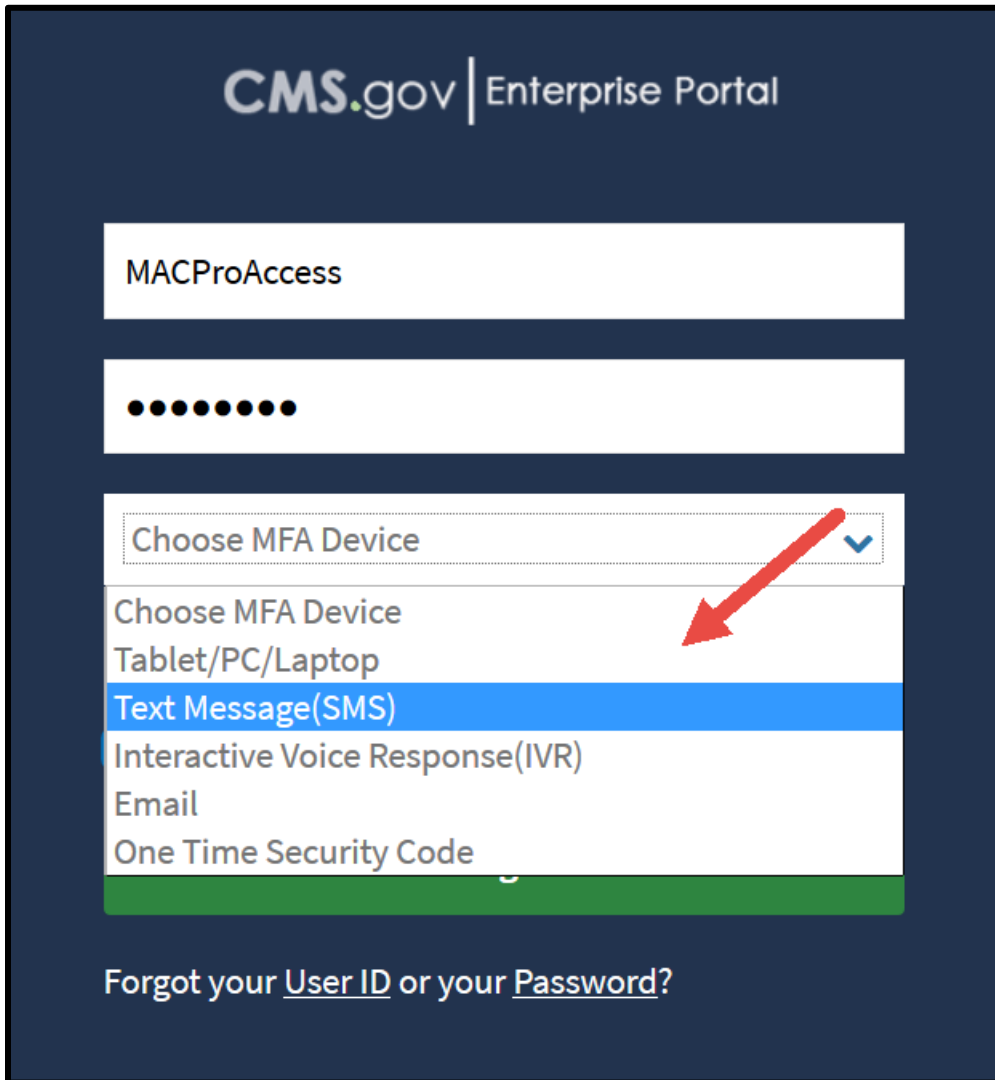
Figure 35: Choose MFA Device drop-down menu

3. Select the button labeled "**Send MFA Code**". Once you receive your code, enter it into the text box labeled "**Enter security code**".

Figure 36: Send MFA Code button and Enter security code field

4. Once you have entered your code, Accept the Terms and Conditions by checking the box in front of "**Agree to our Terms and Conditions**". Then select "**Login**".

Figure 37: Agree to our Terms and Conditions checkbox and Login button

Additional Actions

Forgot User ID

1. Go to the CMS Enterprise Portal Homepage at portal.cms.gov. Select "**Forgot User ID?**" in the CMS Secure Portal box.
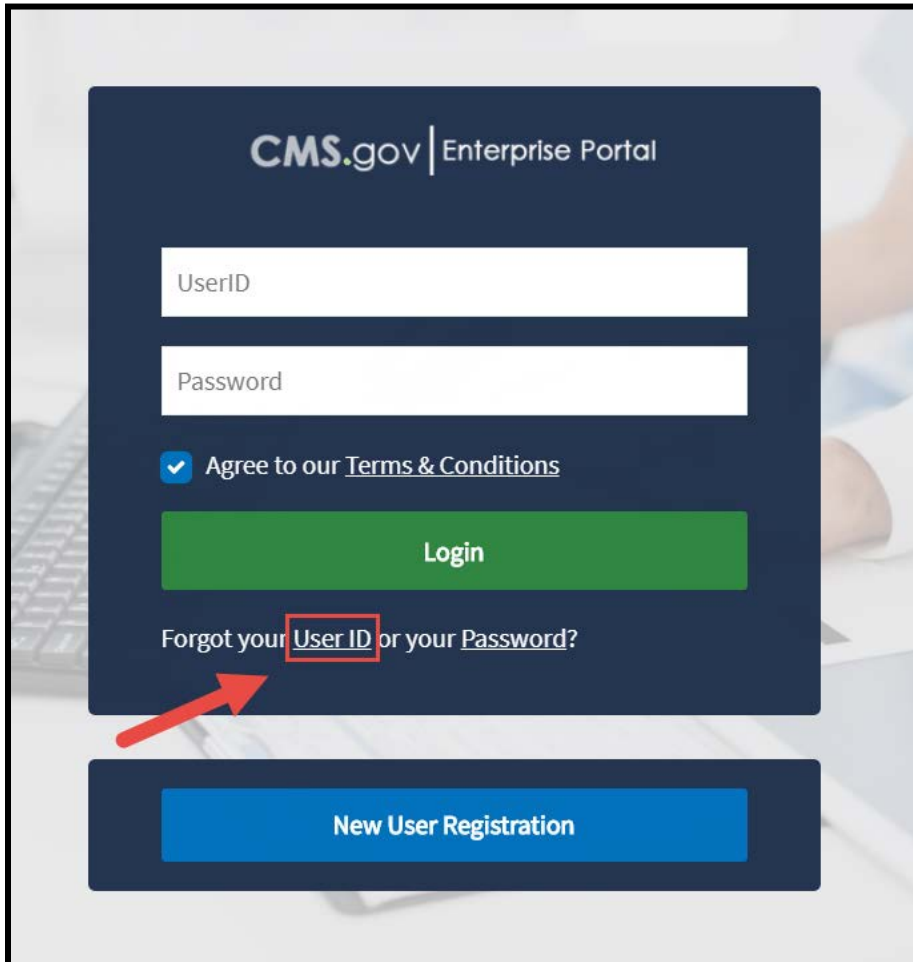
Figure 38: Forgot User ID link

2. Next, enter the information requested and select "**Submit**".

Figure 39: Forgot User ID screen and Submit button

3. If your information is successfully verified, you will receive a notification. Select "**Ok**".

Figure 40:Verification message

4. You will receive an email that will indicate your User ID.
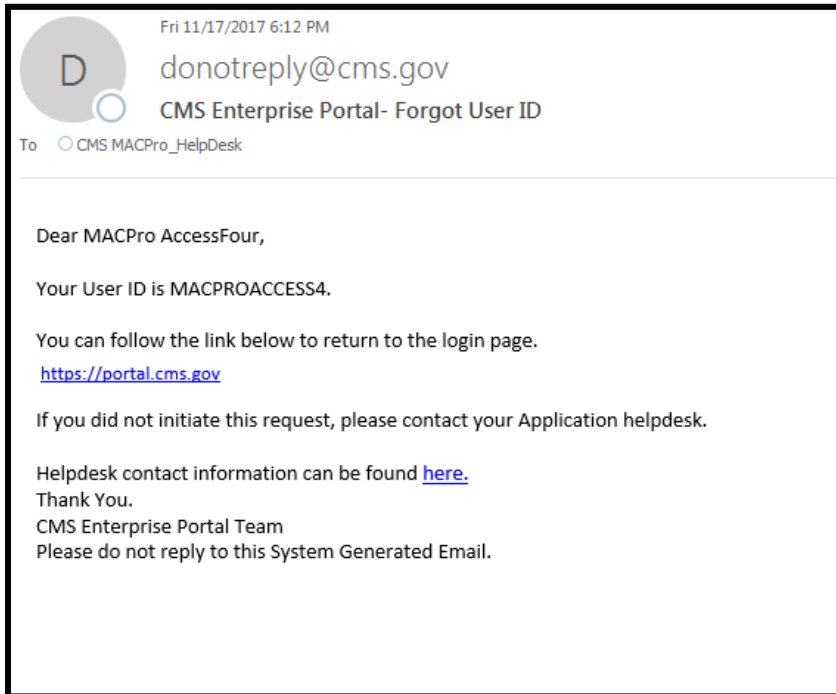
Figure 41:Email message indicating User ID

5. If your information is not successfully verified, you will receive an error message. In this case, proceed to register for an EIDM ID by following the instructions in Step 1. If you believe that you already have an EIDM ID but are entering incorrect information, please contact the MACPro Help Desk at MACPro_HelpDesk@cms.hhs.gov.

Figure 42: Error message indicating invalid data

Forgot Password

1. Go to the CMS Enterprise Portal Homepage at portal.cms.gov. Select "**Forgot Password?**" in the CMS Secure Portal box.
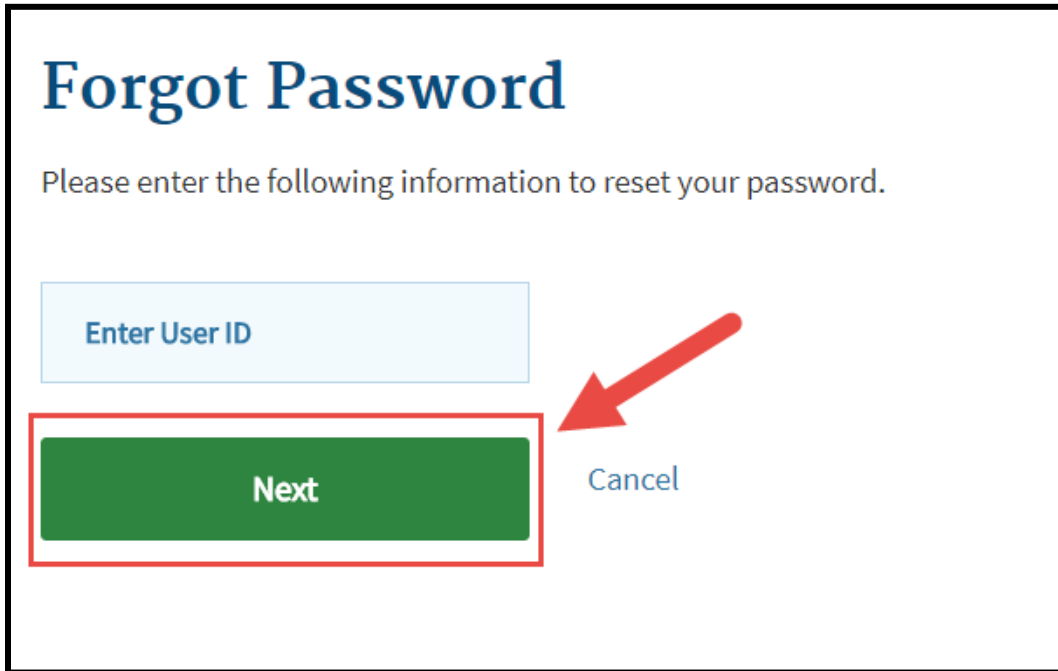
Figure 43: Forgot Password link

2. Next, enter your User ID into the text field and select **"Next".**

Figure 44: Next button

3. Answer the challenge questions and enter in a new password. Then, select "**Submit**". If you do not know your challenge question answers, please contact the MACPro Help Desk at MACPro_HelpDesk@cms.hhs.gov. Please note that your new password must meet the following requirements:

- It must be changed every 60 days
- It must be a minimum of 8 and a maximum of 20 characters
- It can be changed only once every 24 hours
- It must contain at least 1 letter and 1 number
- It must contain at least 1 upper case and 1 lower case letter
- It must contain at least 1 special character
- It must be different than previous passwords used
- It may **not** contain the User ID
- It may **not** contain commonly used words
- The following special characters may **not** be used ? < > ( ) ' " / \ &.

Figure 45: Forgot Password screen and Submit button

Removing an MFA Device

Please Note: While MFA is not required for MACPro, it may be required for other applications within the EIDM Portal. If you have access to another application within the EIDM Portal, please check with the application's help desk before removing MFA from your account.

1. Once logged into the EIDM Portal https://portal.cms.gov navigate to the drop-down menu under your username in the top banner. Select "**My Profile**".
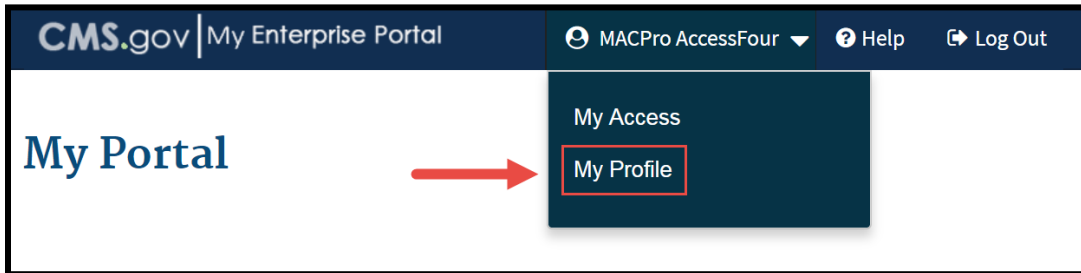
Figure 46: My Profile link

2. Next select the link to "**Remove MFA**" from the left panel.
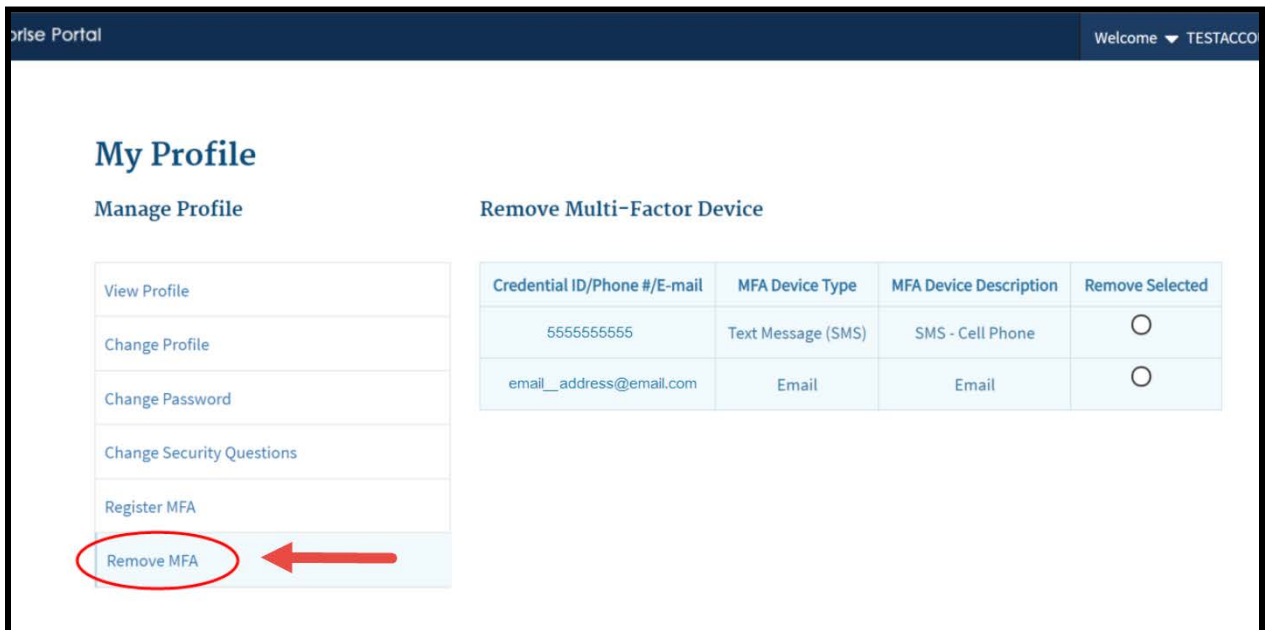
Figure 47: Remove MFA link

3. Then select the radio button next to the device(s) you would like to remove. Then select Send Code to receive the security code for the device. Enter the security code and select "Remove Device".
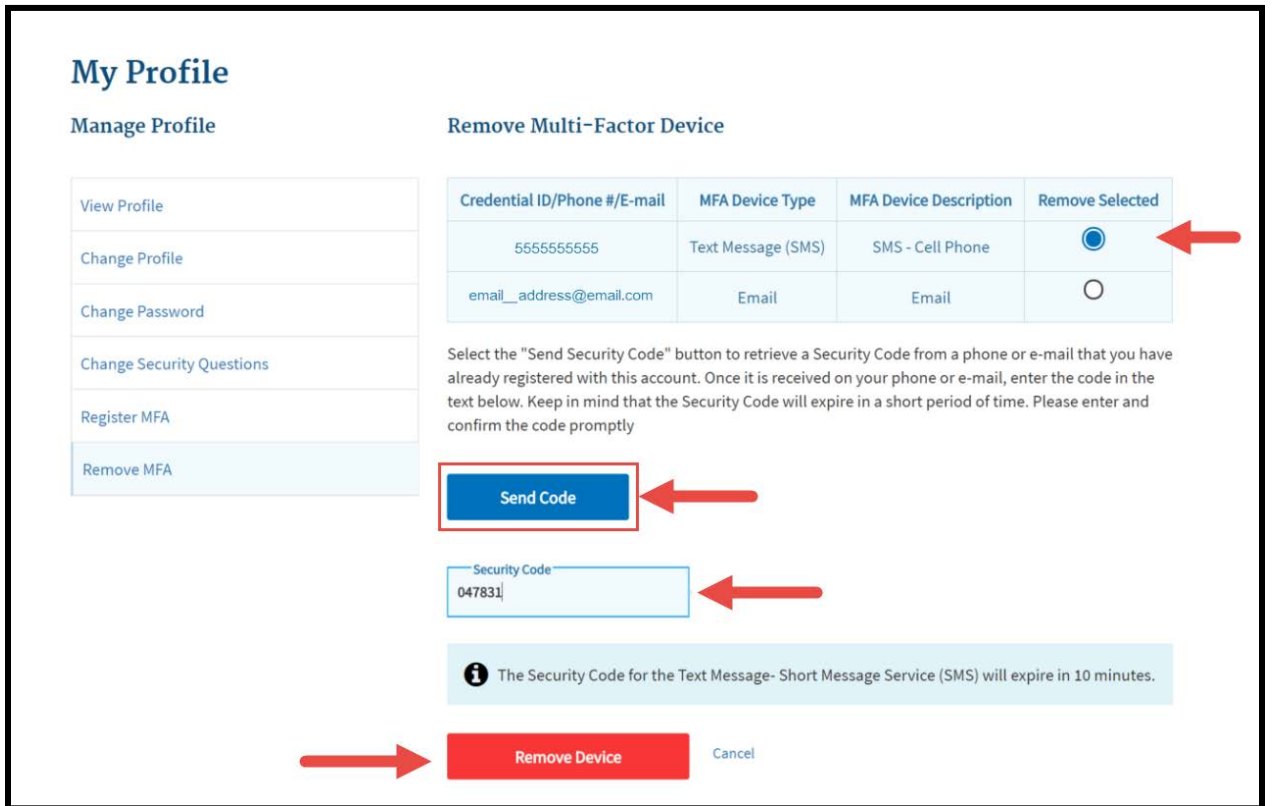
Figure 48: Remove Multi-Factor Device screen

4. After selecting "Remove Device" a confirmation message will appear stating "Changes to your profile have been successfully submitted."

Figure 49: Confirmation message

Cancel a Pending Role Request in EIDM

1. Once logged into the EIDM Portal https://portal.cms.gov navigate to the drop-down menu under your name in the top banner. Select "**My Access**".
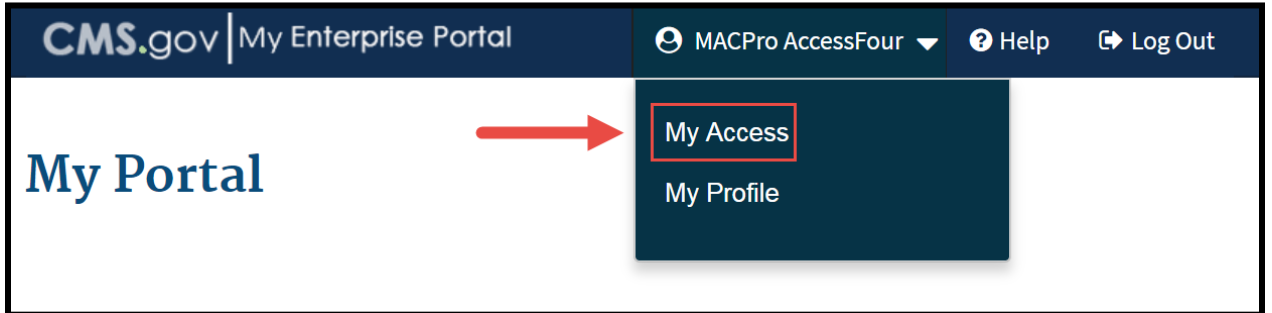
Figure 50: My Access link

2. Scroll down to the My Pending Requests box. Select the linked Request ID.
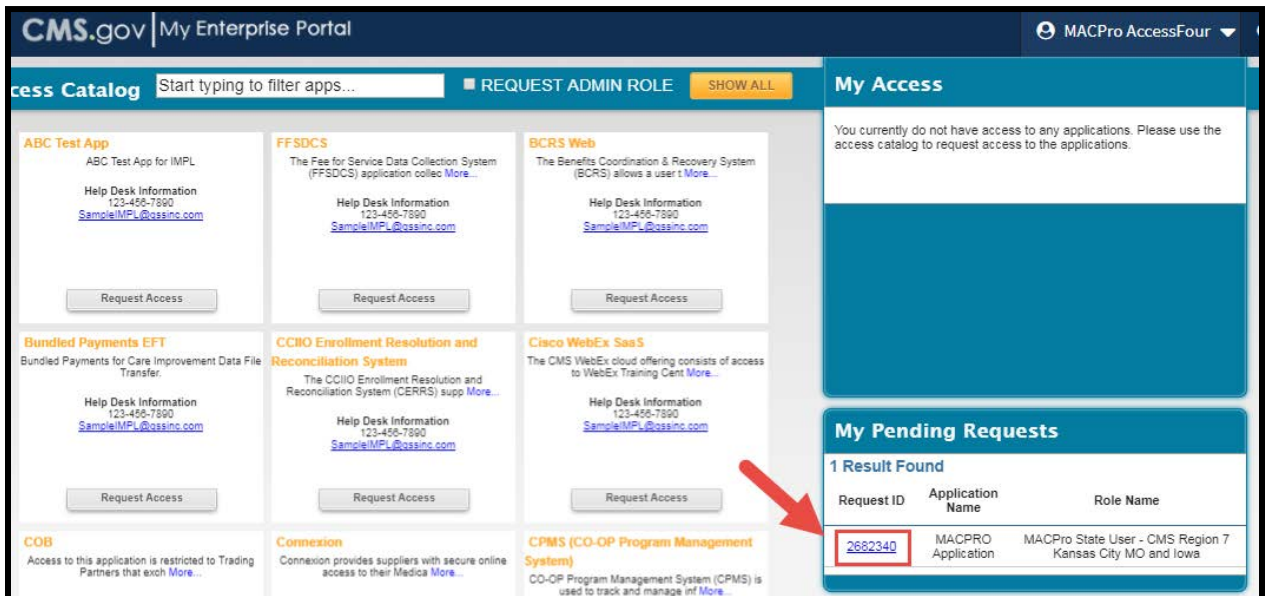
Figure 51: Request ID link

3. Select "**Cancel**" from the Pending Requests table.
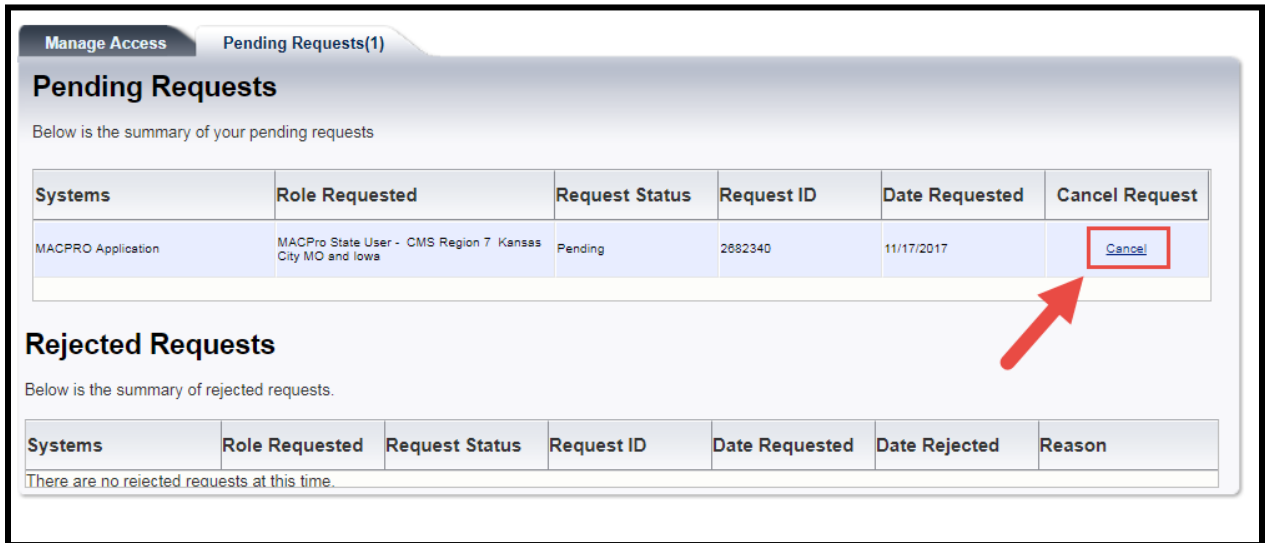
Figure 52: Cancel Request link

4. Select "**Submit**"
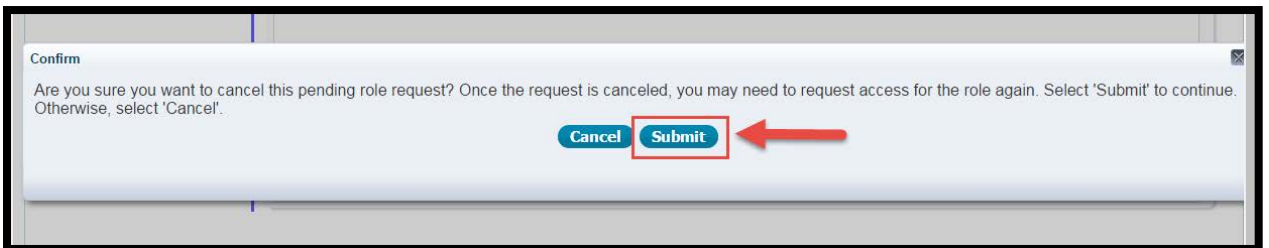
Figure 53: Submit button

5. A confirmation will show in a blue banner indicating you have successfully canceled your request.
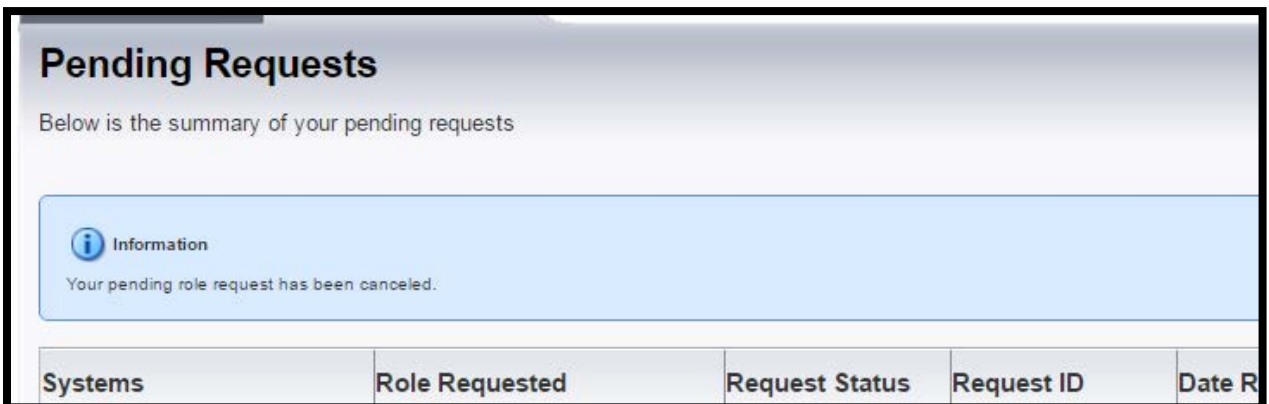
Figure 54: Confirmation message indicating request has been canceled

Subscribe to EIDM Portal Notifications

Subscribing to EIDM Portal notifications will provide you with helpful general system updates related to the EIDM Portal such as potential system issues, upgrades, new features, etc. This is optional and is not specific to MACPro.

1. Navigate to the EIDM Portal (https://portal.cms.gov) and select the button on the top right of the screen labeled **"Email Alerts"**.
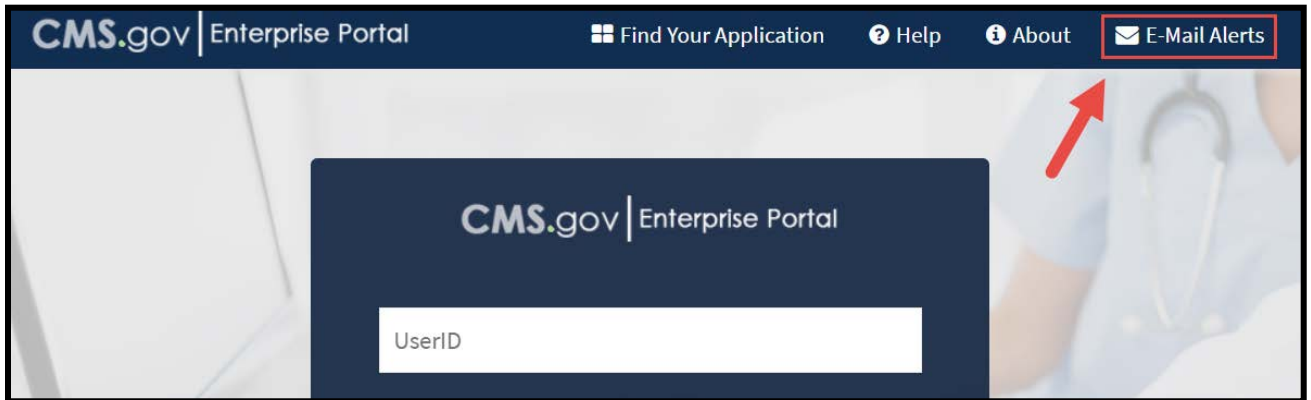
Figure 55: E-mail Alerts link

2. Enter in your email address and then click "**Submit**".
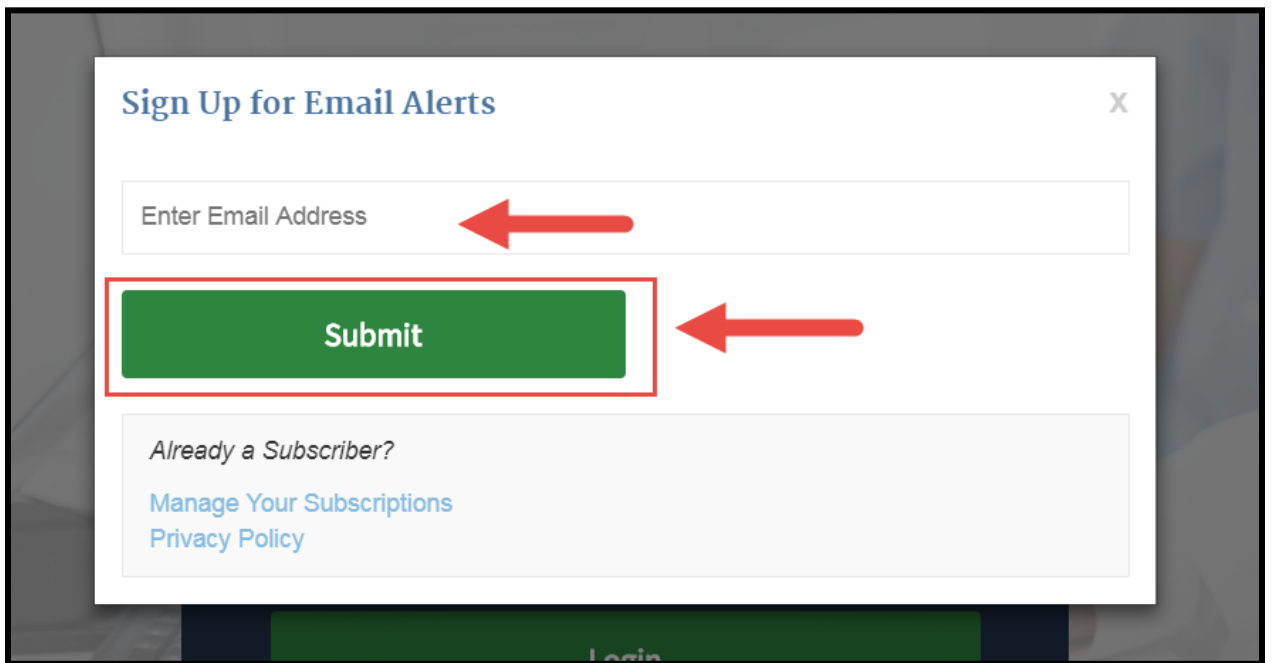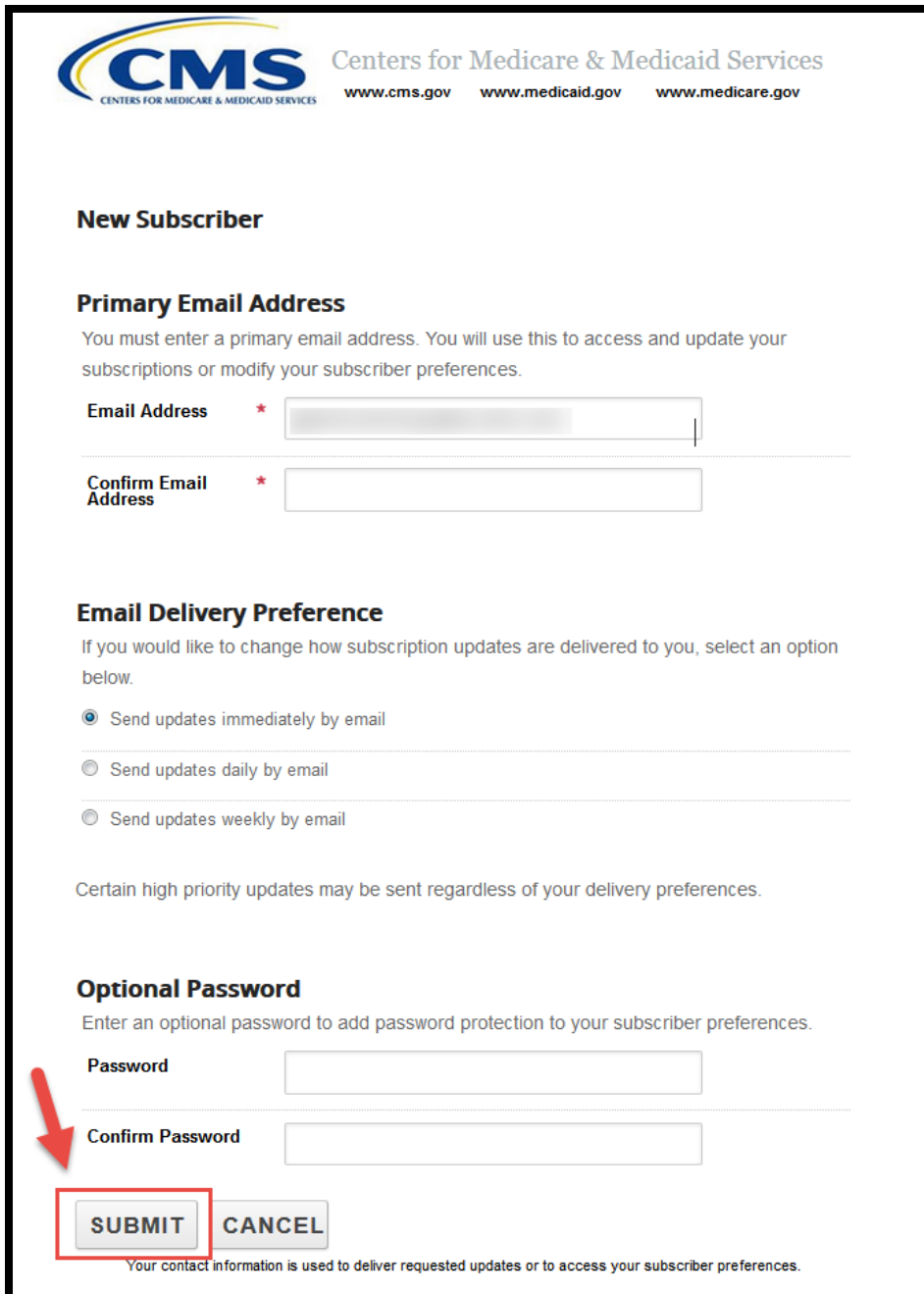
Figure 56: Enter Email Address field and Submit button

3. Confirm your email address, determine the frequency in which you would like to receive notifications, and determine whether you would like to have a password on your subscriber preferences. After completing these steps, select "**Submit**".

Figure 57: New Subscriber screen and Submit button

4. You will then receive confirmation that you have successfully registered for notifications. By selecting "**Subscriber Preferences**" you can determine which notifications you are subscribing to. If you do not wish to update your preferences, select "**Finish**".
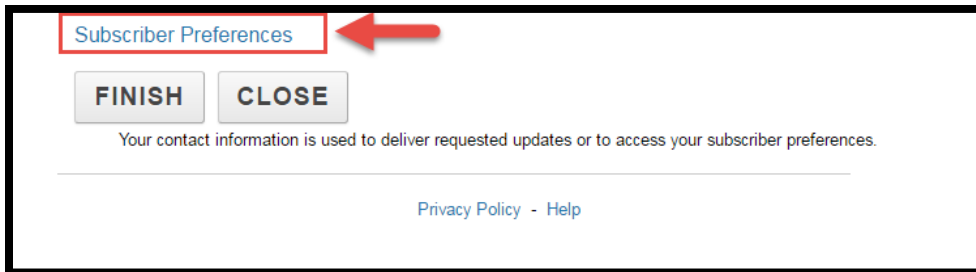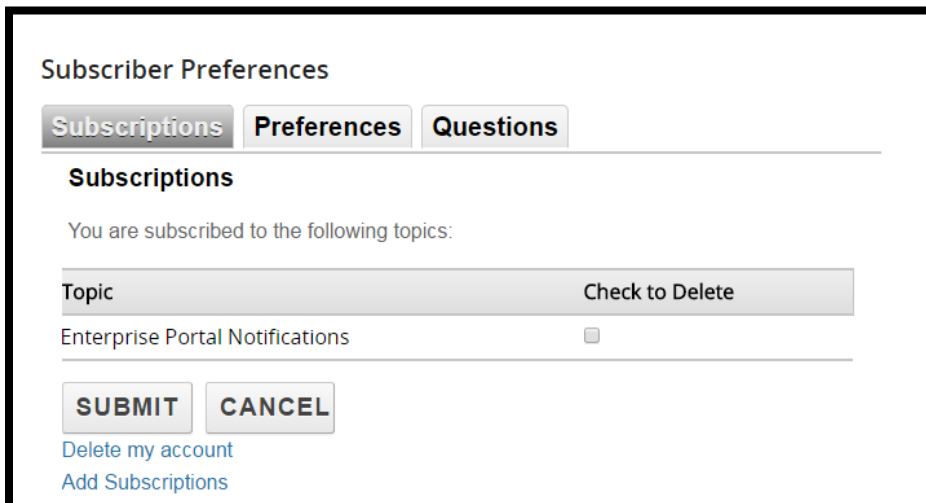

Figure 58: Subscriber Preferences link

Figure 59: Subscriptions tab

Figure 60: Finish button

Change Password

1. Once logged in to the CMS Enterprise Portal, select "**My Profile**" in the drop down menu under your name in the top banner.
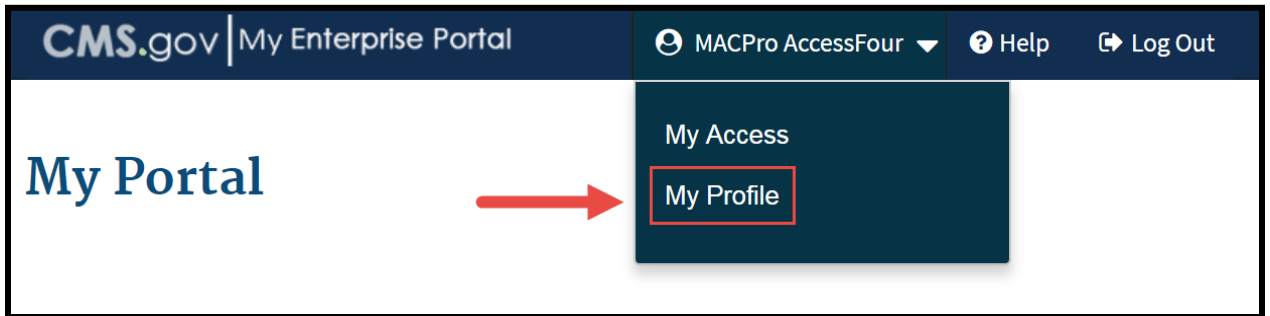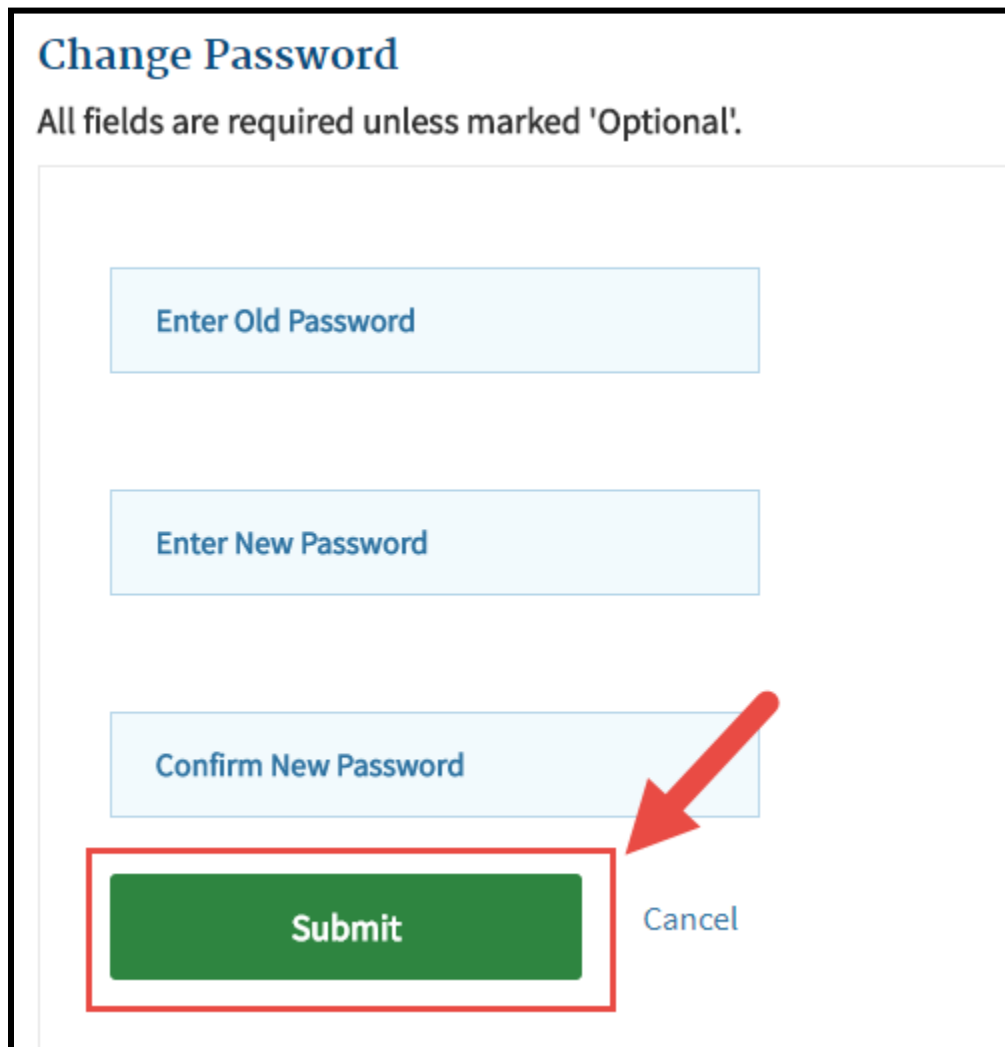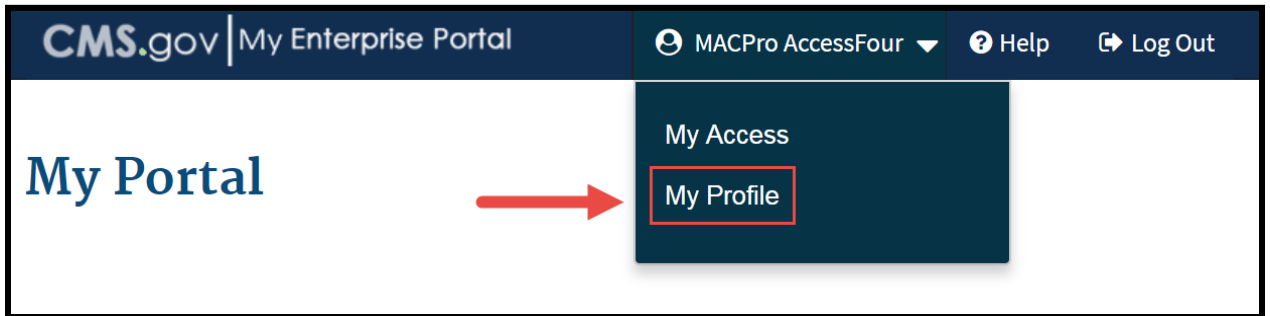

Figure 61: My Profile link

2. Next, select "**Change Password**".

Figure 62: Change Password link

3. Enter your Old Password, and then your New Password. Then select "**Submit**"
   - It must be changed every 60 days
   - It **must** be a minimum of 8 and a maximum of 20 characters
   - It can be changed only once every 24 hours
   - It must contain at least 1 letter and 1 number
   - It must contain at least 1 upper case and 1 lower case letter
   - It must contain at least 1 special character
   - It must be different than previous passwords used
   - It may **not** contain the User ID
   - It may **not** contain commonly used words
   - The following special characters may **not** be used ? < > ( ) ' " / \ &.

Figure 63: Submit button

4. You will receive a confirmation message stating that "Changes to your profile have been successfully submitted".

Figure 64: Confirmation message indicating changes to profile have been submitted

5. The next steps you will take are the requesting an EIDM role for MACPro. Please follow the instructions in Step 2 for requesting a role.

Change Challenge Questions

1. Once logged in to the CMS Enterprise Portal, select "**My Profile**" in the drop-down menu under your name in the top banner.

Figure 65: My Profile link

2. Select "**Change Challenge Questions**".

Figure 66: Change Challenge Questions link
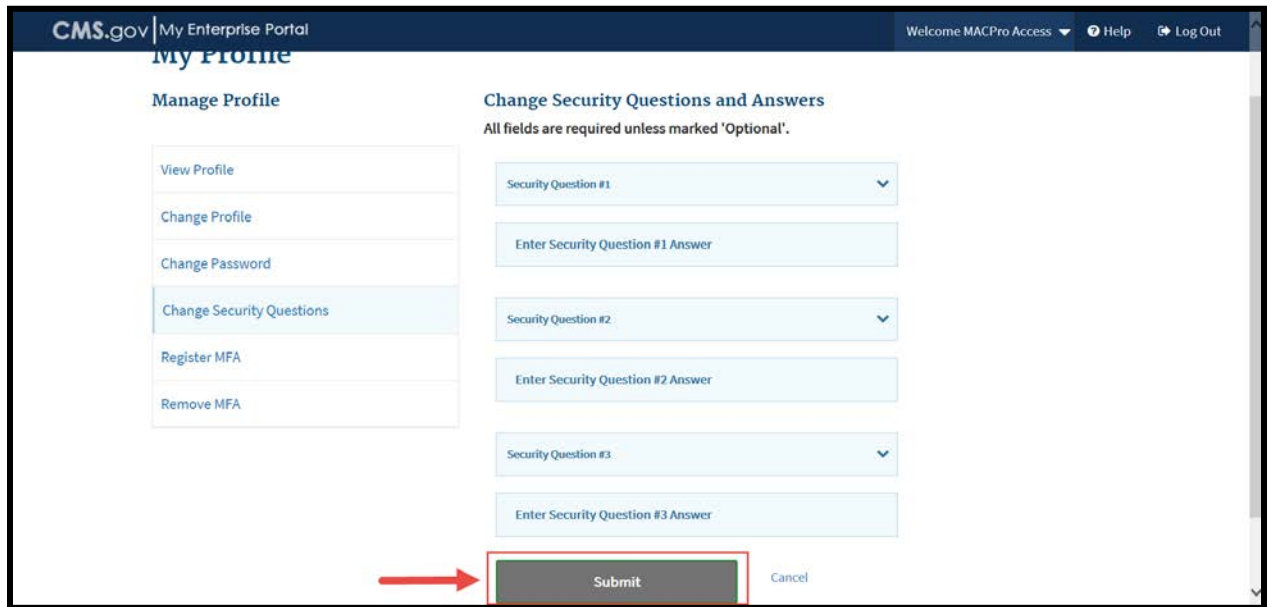
3. Enter your User ID and Password. Select "**Next**".

Figure 67: Change Challenge Questions screen and Next button

4. Create challenge questions and answers that you will remember in the future. This is important as you will answer these challenge questions when a password reset is required. Select challenge questions and answers, then select "**Submit**".

    Please note: after you populate all fields, you must click outside the box for the "**Submit**" button to become active.

Figure 68: Submit button

5. You will receive a confirmation message stating that "Changes to your profile have been successfully submitted".
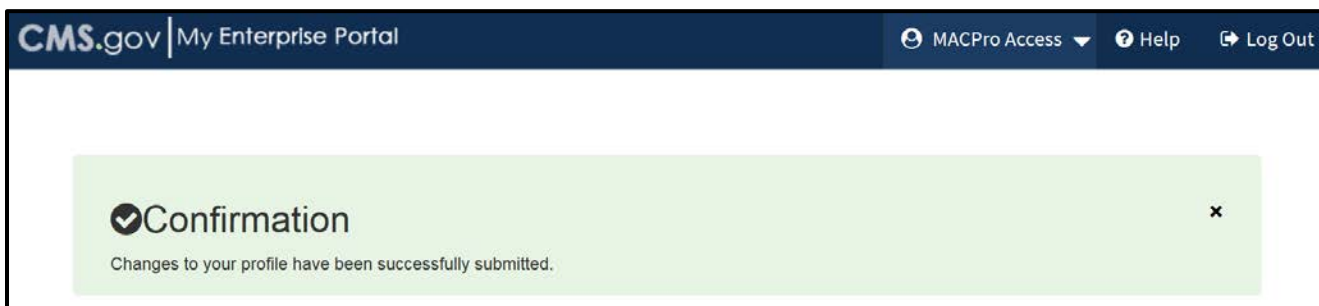

Figure 69: Confirmation message indicating changes to your profile have been submitted