Quality Payment
PROGRAM

2017 Medicare Shared Savings Program Accountable Care Organization (ACO) Quality Reporting Guide: Enterprise Identity Data Management (EIDM) Account and Role Set Up

Table of Contents

Introduction

If your ACO is participating in the Medicare Shared Savings Program (Shared Savings Program) for performance year 2017, then you must set up the necessary Enterprise Identity Management (EIDM) accounts and roles to enter and submit quality data through the CMS Web Interface (CMS WI). The CMS WI will be accessible through the Quality Payment Program (QPP) Portal that will be available on the QPP website and announced through the ACO Spotlight Newsletter.

As required by the Shared Savings Program, ACOs must completely and accurately report all quality measures to meet the quality performance standard. ACOs who do not meet the quality performance standard will not be eligible to share in savings, if earned. In addition, the QPP will use the ACO reported CMS WI data to calculate the Quality performance category for all Merit-based Incentive Payment System (MIPS) eligible clinicians participating in the ACO. For more information on the interactions between the Shared Savings Program and the QPP, please visit the Fact Sheet available in the QPP Resource Library.

Your ACO will not be able to meet the complete and accurate quality reporting requirements without Quality Payment Program Portal access, which is obtained through CMS Enterprise Portal. **EIDM accounts are NOT the same as the CMS User IDs (EUA accounts) that are issued to ACO contacts and needed to access the Shared Savings Program ACO Portal. Users cannot use their CMS User ID for quality reporting and must create EIDM accounts and roles.**

EIDM accounts will enable your ACO to:

- Access the QPP Portal;
- Access the CMS WI to download your Beneficiary Sample prior to the CMS WI data submission period;
- Access the CMS WI training environment; and
- Enter and submit quality data via the CMS WI during the submission period to fulfill program requirements for complete and accurate reporting.

ACOs must have all of their EIDM accounts and roles established by January 2018 to be able to access the CMS WI and be ready for quality reporting.

EIDM Accounts and Roles Overview

In order to report CMS WI data, each ACO must have individuals with the ACO Security Official (ACO SO) and Web Interface Submitter roles within the EIDM **Physician Quality and Value Programs Application**. In order to access the EIDM Physician Quality and Value Programs Application to request the ACO SO and Web Interface Submitter roles, individuals will need to first create an EIDM account. The table below provides important information describing each role needed for CMS WI quality reporting.

Role	Responsibilities	Approval
ACO Security Official (ACO SO)	User must be from the ACO and approves Web Interface Submitter role requests. The ACO SO validates the users who can access the CMS WI and report quality data. The ACO SO has access to the CMS WI to download the Beneficiary Sample, participate in the training environment, enter and submit quality data, and generate reports. *All users must be in the United States of America.	Requests may be automatically approved in the system when requesting the ACO SO role. Individuals have 3 attempts to submit their ACO SO role request with accurate information. After 3 failed attempts, the request will be sent to the Quality Payment Program Service Center for manual approval. Please contact the QPP Service Center at qpp@cms.hhs.gov for assistance. ACOs may have more than 1 ACO SO. We recommend having more than 1 ACO SO, in case your ACO SO is out of the office or unable to approve WI Submitters.

Role	Responsibilities	Approval
Web Interface Submitter	User has access to the CMS WI, through the QPP Portal, to download the Beneficiary Sample, participate in the training environment, enter and submit quality data, and generate reports. *Third party vendors may be a Web Interface Submitter, but all users must be in the United States of America.	The ACO SO must approve Web Interface Submitter requests.

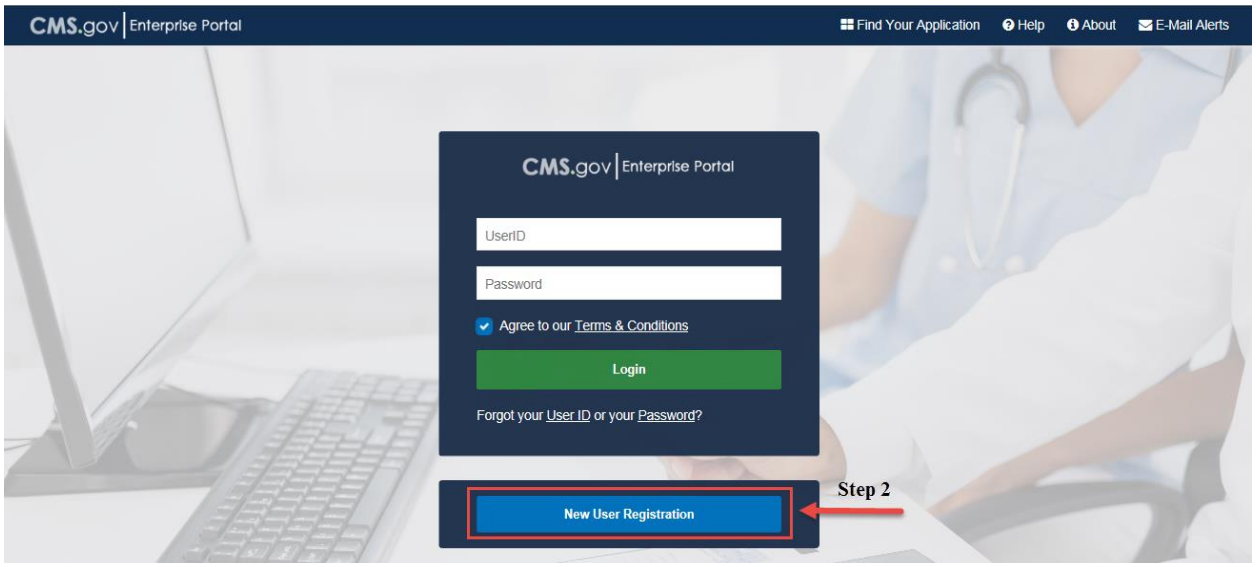
How to Register and Create EIDM Accounts

If you already have an active EIDM account, then you do not need to set up a new EIDM account. Please note screenshots are taken from a test environment and may not display exactly what you see on your screen.

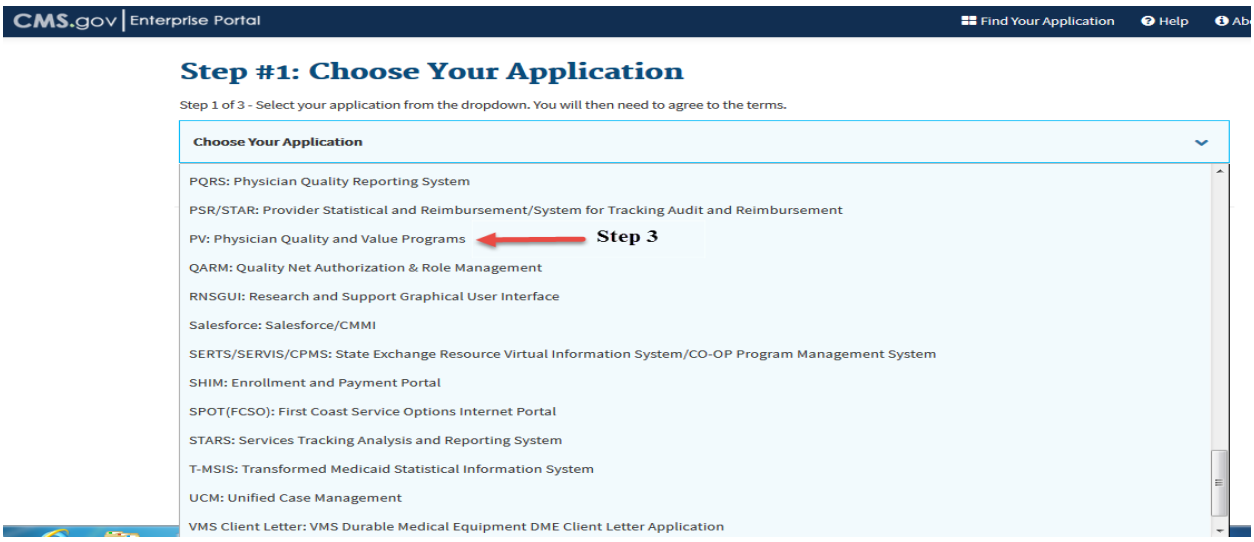
Steps for Creating a New EIDM Account:

1. Navigate to https://portal.cms.gov/.
   The CMS Enterprise Portal page is the same website used to access the ACO Portal, but your CMS user ID for the ACO Portal will not give you the access you need to request roles. Please create an EIDM account if you do not have one or use your existing EIDM account to request the necessary roles.

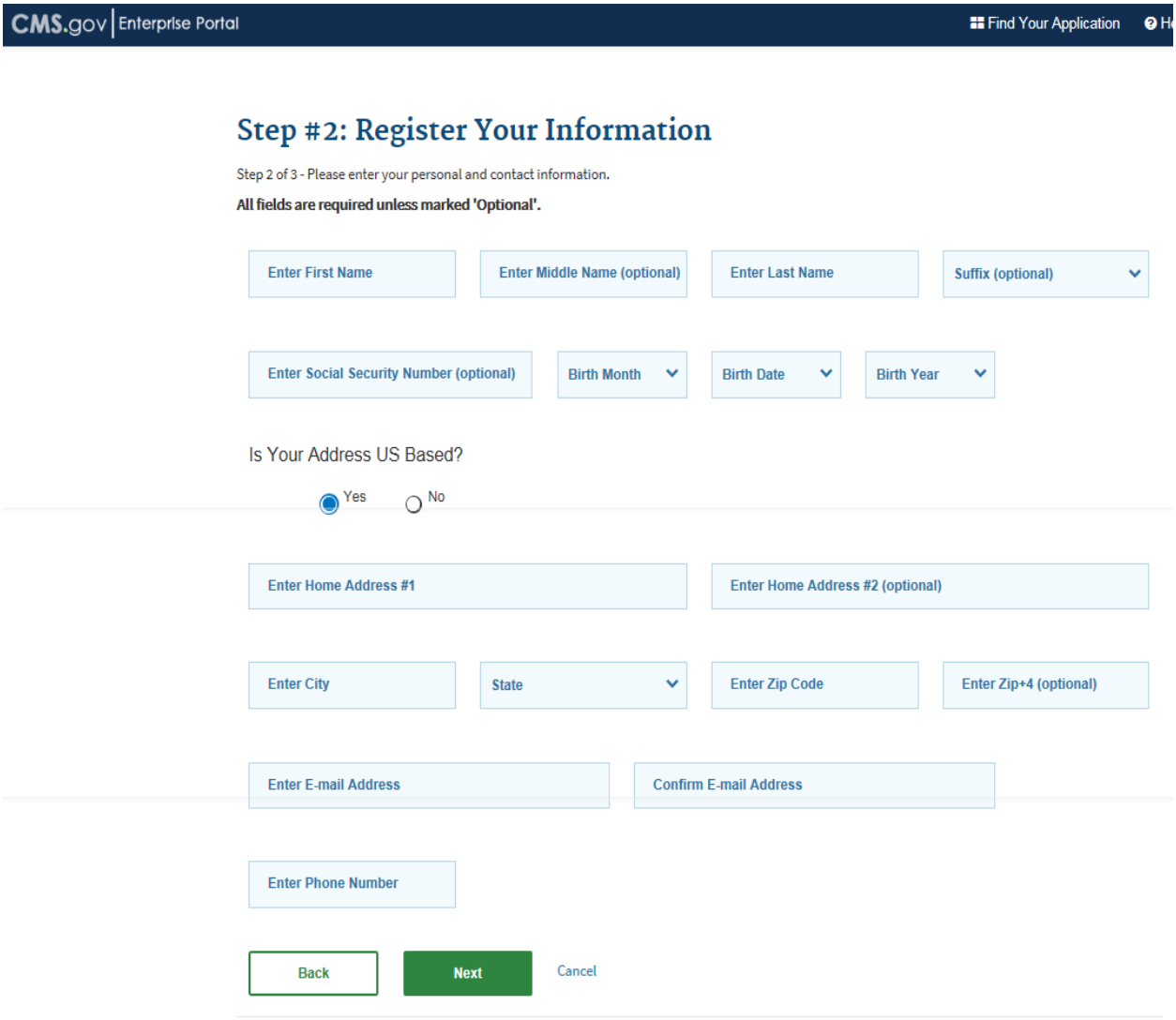
2. Select the '**New User Registration'** link.



3. Select **Physician Quality and Value Programs** application from the dropdown menu and agree to the terms and conditions.



4. The **'Register Your information'** page is displayed. Provide the information requested on the **'Register Your Information'** page. The fields with an asterisk (*) are required fields and have to be completed. After all required information has been provided, select **'Next'** to continue.



NOTE: You may select '**Cancel**' at any time to exit out of the user ID registration process. All information provided, and any changes made, will not be saved.

After providing the required information on the **'Register Your Information'** page, the **'Create User ID, Password & Security'** page is displayed.

5. **Create and enter a user ID** of your choice and based on the requirements for creating a user ID.

6. **Create and enter a password** of your choice. Enter the same password for 'Confirm Password'. The passwords must match before you can continue.

   NOTE: Please follow the following rules for setting up a user ID and password:

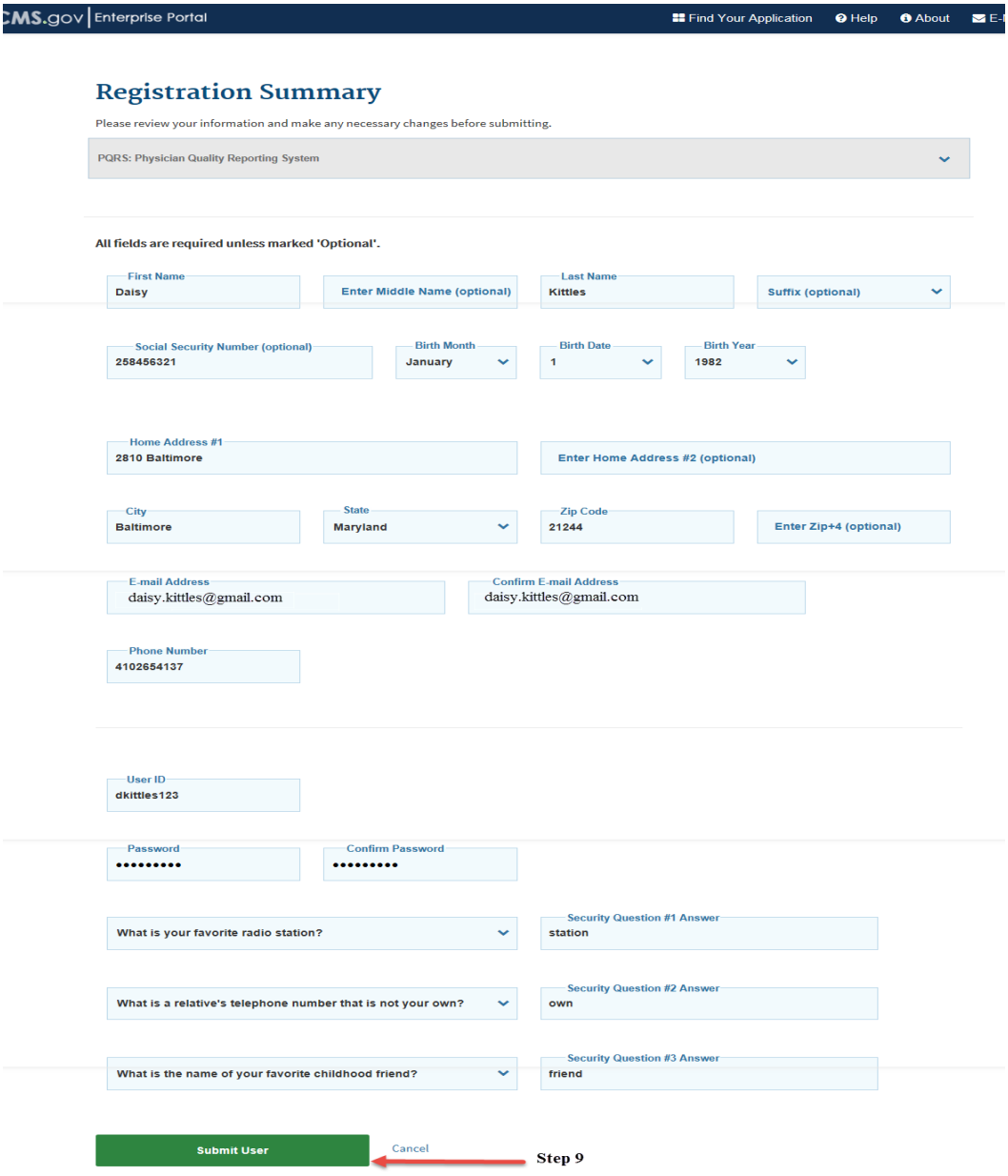
   - **USER ID:** Your user ID must: Be a minimum of 6 and a maximum of 72 alphanumeric characters – Contain at least 1 letter – Cannot contain your Social Security Number (SSN) or any 9 consecutive numbers – Allowed special characters are dashes (-), underscores (_), apostrophes ('), @ and periods (.), followed by alphanumeric characters.
   - **Password:** Your password must be a minimum of 8 and a maximum of 20 characters long. It must contain at least 1 letter, 1 number, 1 uppercase letter, and 1 lowercase letter. It cannot contain your user ID.

7. In the '**Select Security Questions and Answers'** section, select a question of your choice and enter the answer you want to be saved with the question. Repeat for questions 2 and 3.

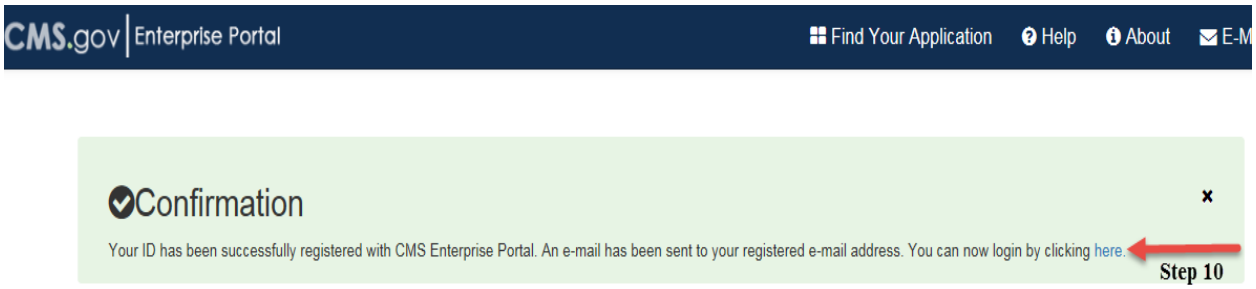
NOTE: You may select '**Cancel**' at any time to exit out of the user ID registration process. All information provided, and any changes made, will not be saved.

8. Select '**Next**' and you will be directed to **Registration Summary** page.

9. The **Registration Summary** page is displayed, review your information and make necessary changes before submitting. Select **Submit User** to complete the registration.



10. **Confirmation** message is displayed with information that your ID has been successfully registered with CMS Enterprise Portal and e-mail has been sent to your registered e-mail address. Select **'here'** to login to CMS Enterprise Portal.



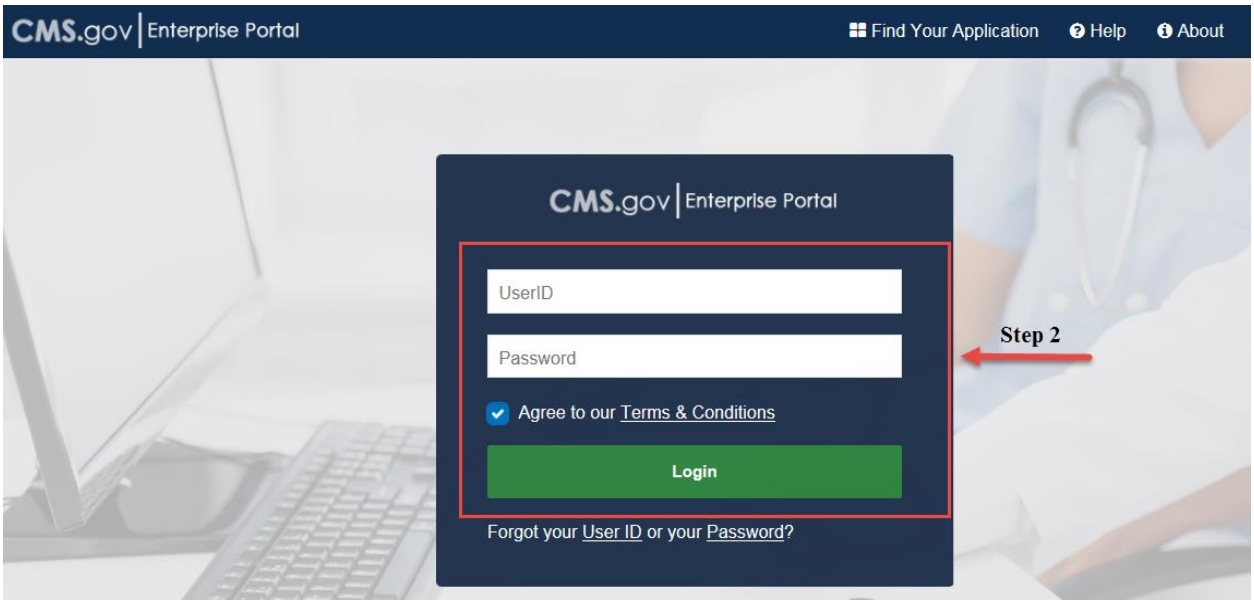
How to Set Up ACO Security Official (SO) Role

After successfully creating an EIDM user ID and password you must set up an ACO SO. If you were previously an ACO SO and maintained an active EIDM account, you can check the status of your role using the instructions provided in the section titled, “How to Check Your Role Status.” Please note screenshots are taken from a test environment and may not display exactly what you see on your screen.

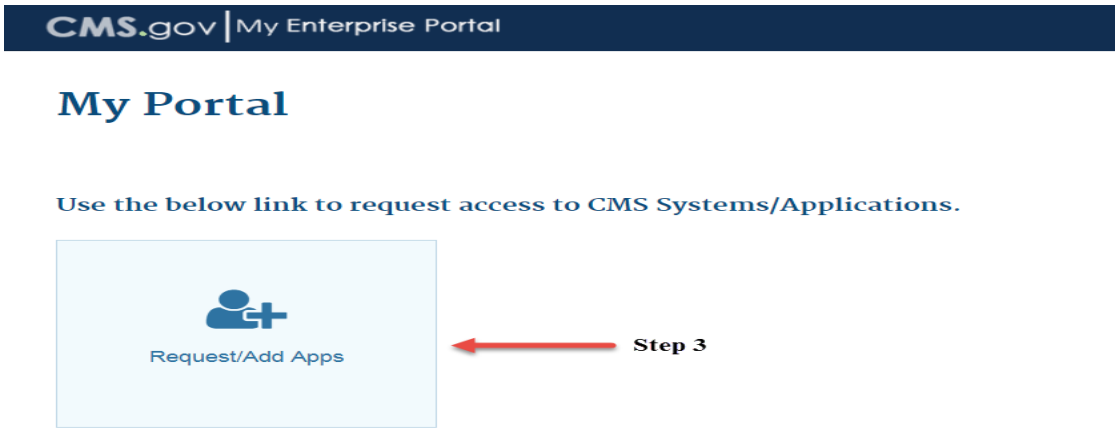
Steps to Create a New ACO SO Role:

1. Navigate to https://portal.cms.gov. The CMS Enterprise Portal home page is displayed.

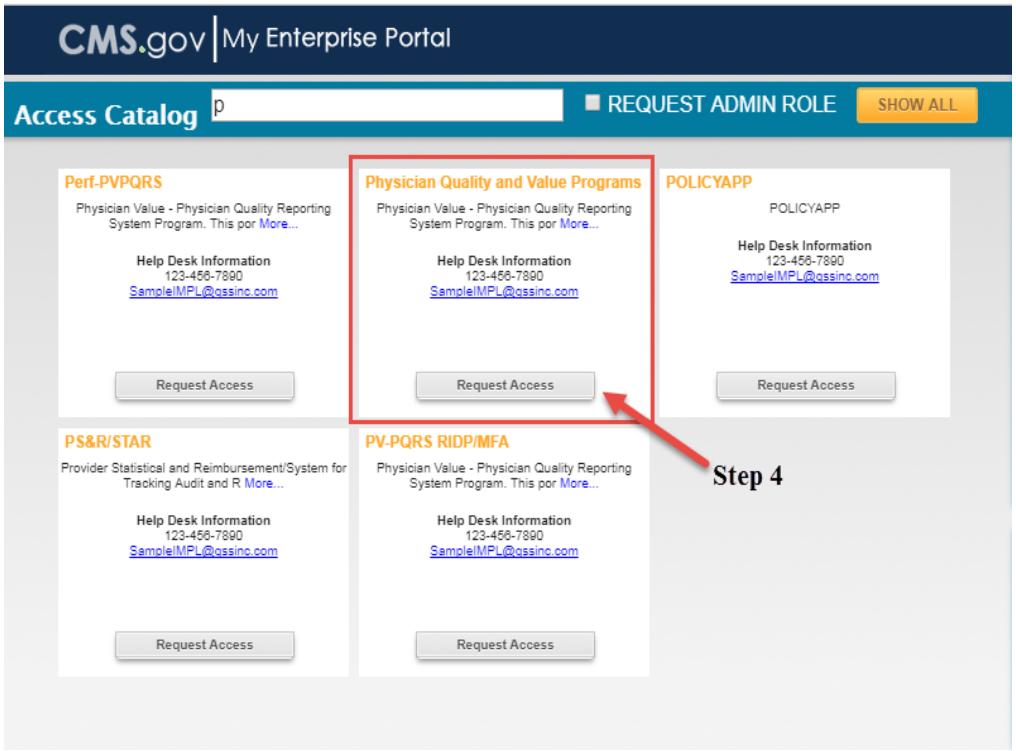
2. Once on the page, enter your user ID and password and agree to Terms and Conditions by clicking the checkbox.



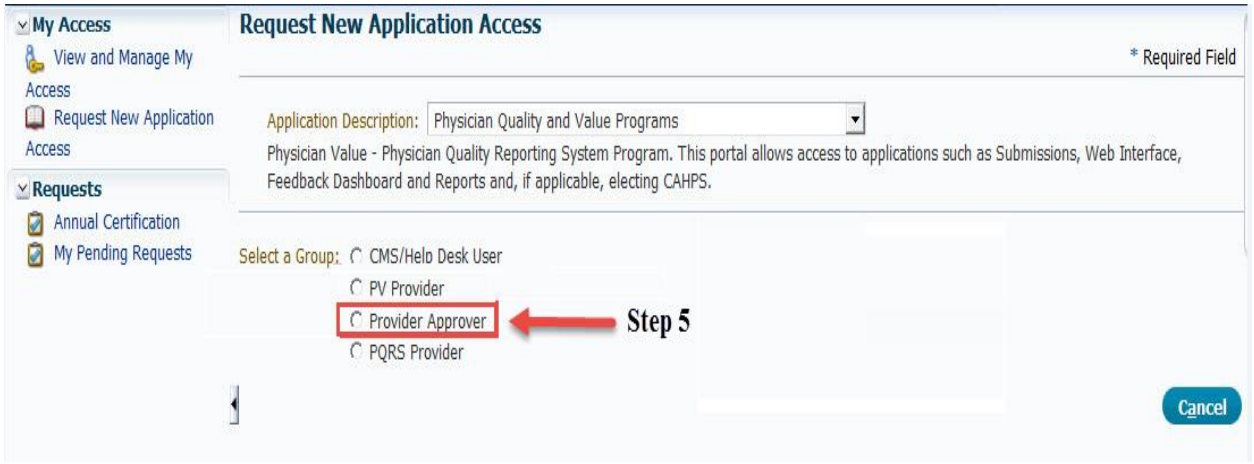
3. The **'My Portal'** page is displayed. Select the **'Request/Add Apps'** link to request access to CMS Systems/Applications.



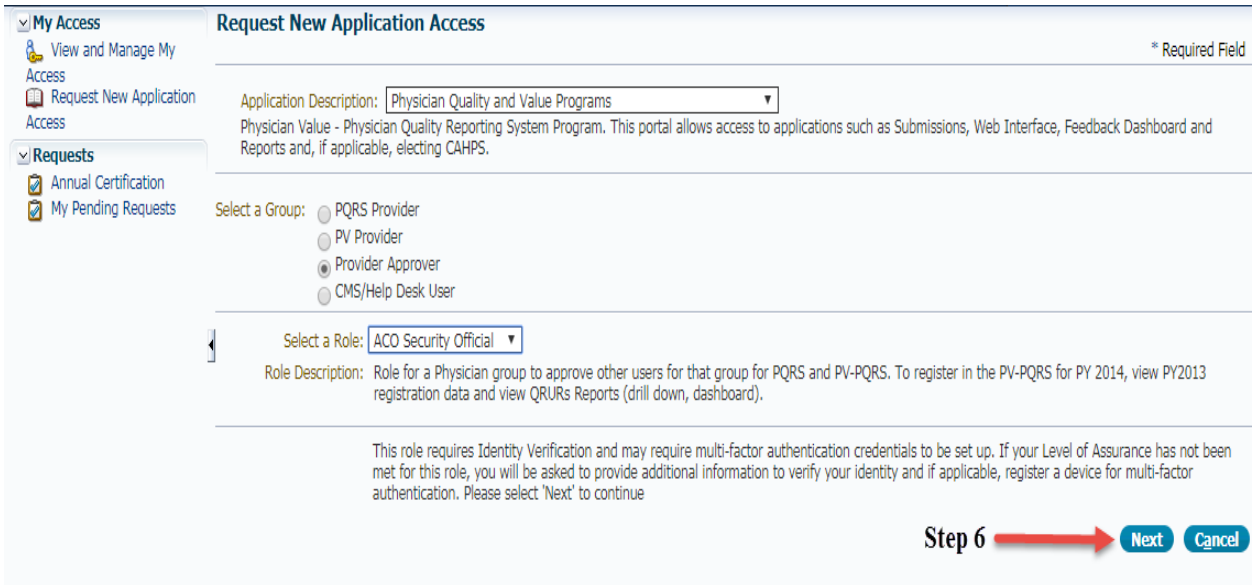
4. For the PQRS and the PV-PQRS Applications; scroll down to the '**Physician Quality and Value Programs**' domain and select **'Request Access.'**



5. At the top of the next screen, the Physician Quality and Value Programs Domain will be auto-populated. Under '**Select a Group**', select '**Provider Approver**.'

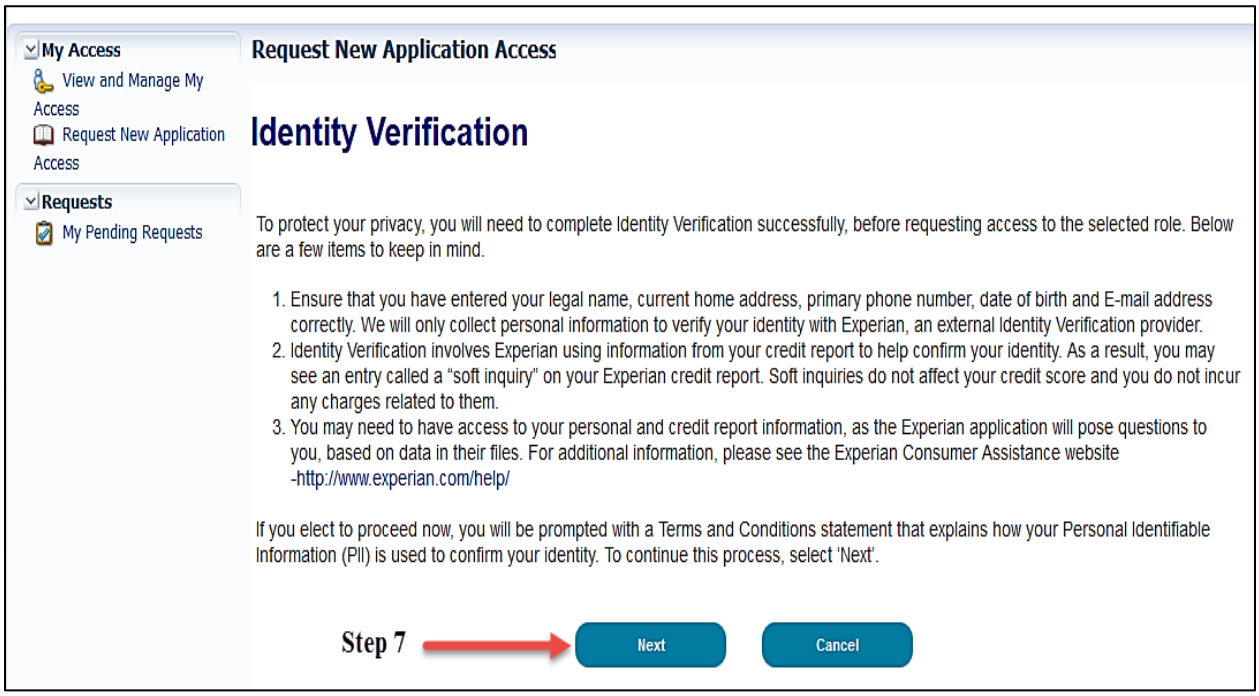


6. Select the appropriate '**Approver Role**' which is the '**ACO Security Official**', then select '**Next**'.

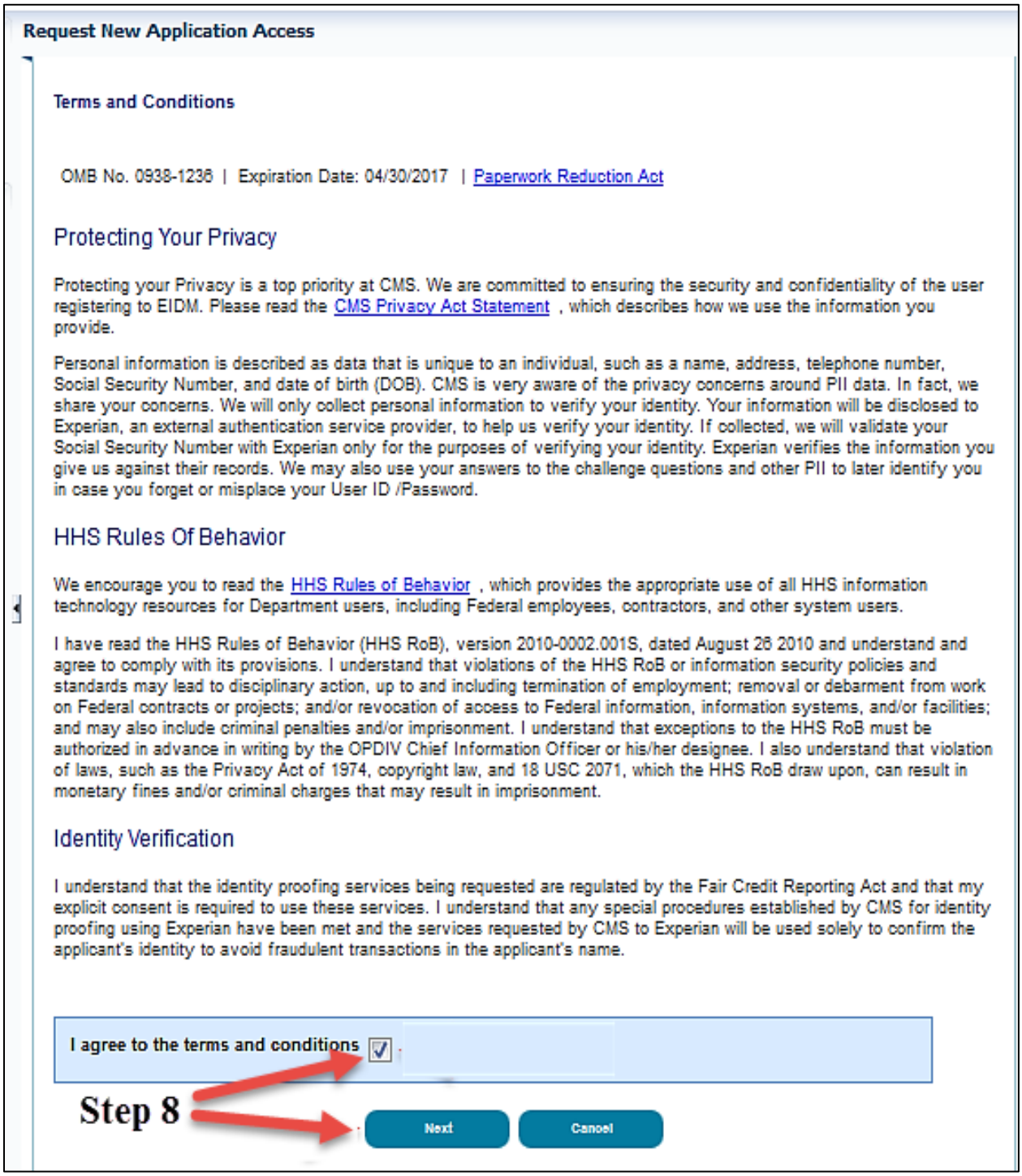


7. Select '**Next**' to complete the '**Identity Verification**' section. The Identity Verification process will only be completed the first time a user requests a role in the Physician Quality and Value Programs domain in EIDM. If the Identity Verification has been completed, users can skip to step 17 to request additional roles.

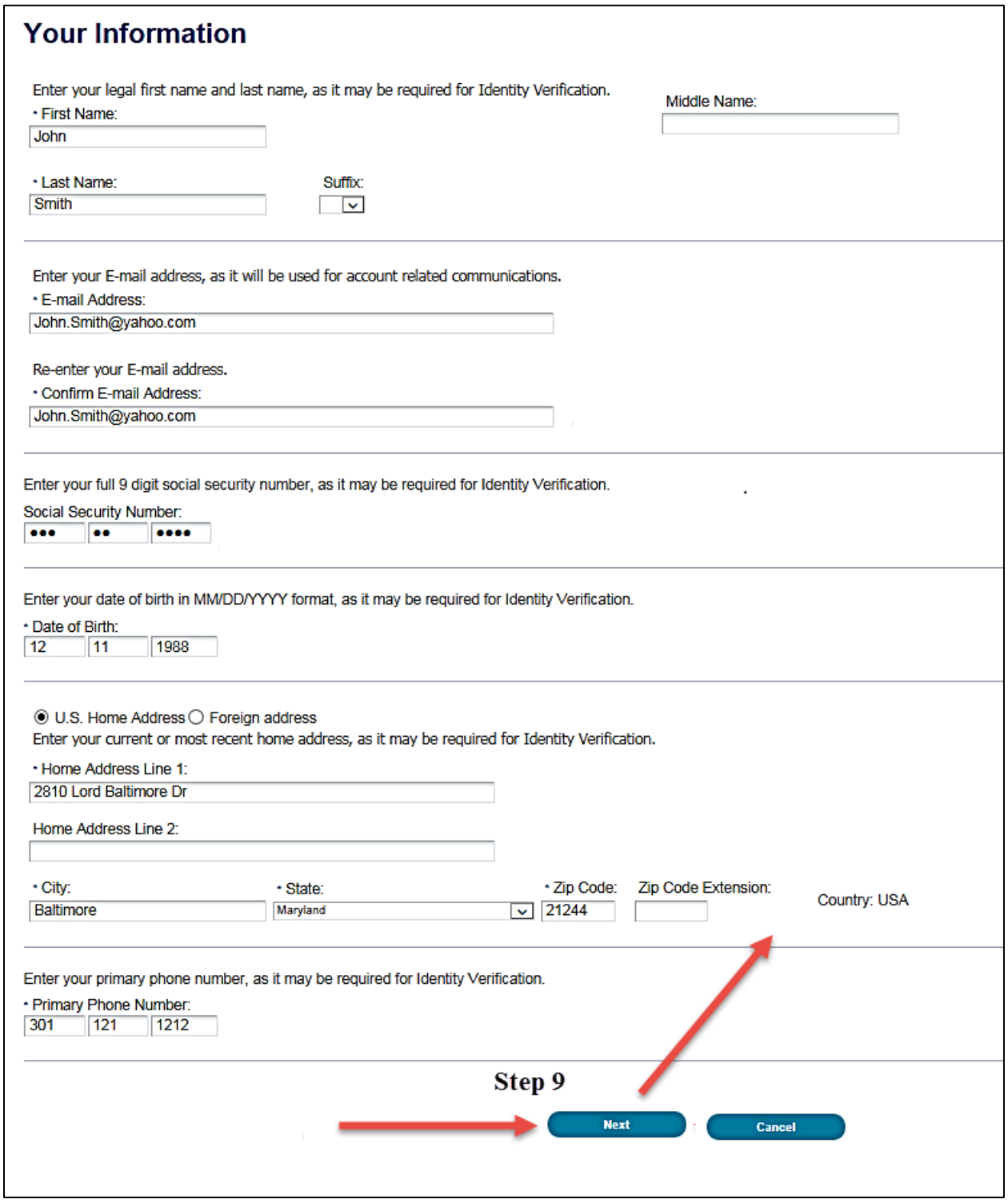
   NOTE: Users must be in the United States of America to complete Identity Verification.



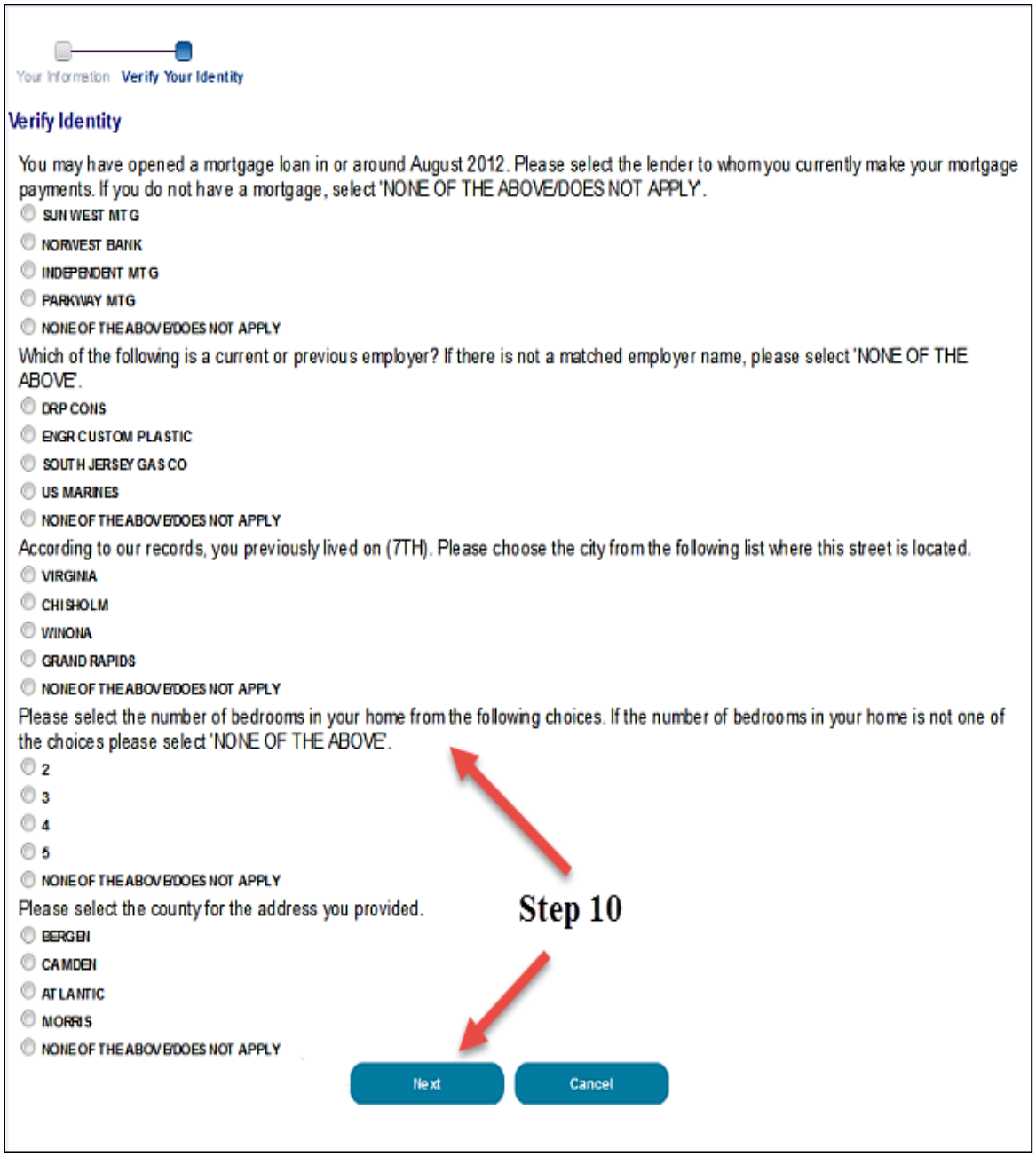
8. Read the Terms and Conditions. Select the '**I agree to the terms and conditions**' checkbox and then select '**Next**'. '**Next**' will be enabled only after checking the '**I agree to the terms and conditions**' checkbox.



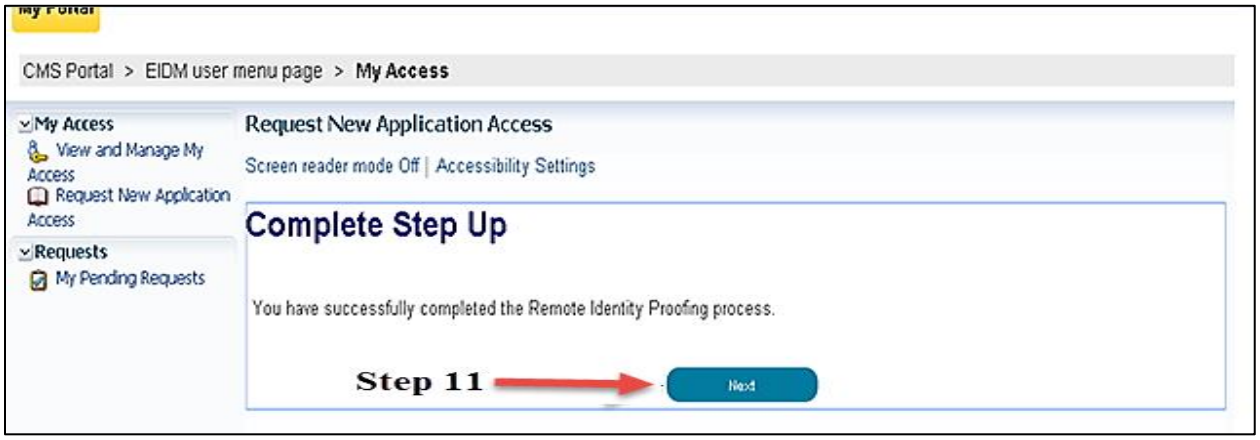
9. Enter the required information under **'Your Information'** section. Select '**Next**' when complete.



10. Select an answer to each question under '**Verify Identity**'. Select '**Next**' after providing an answer to each question. '**Verify Identity**' question information is provided from Experian in association with the SSN Number provided in step 9.

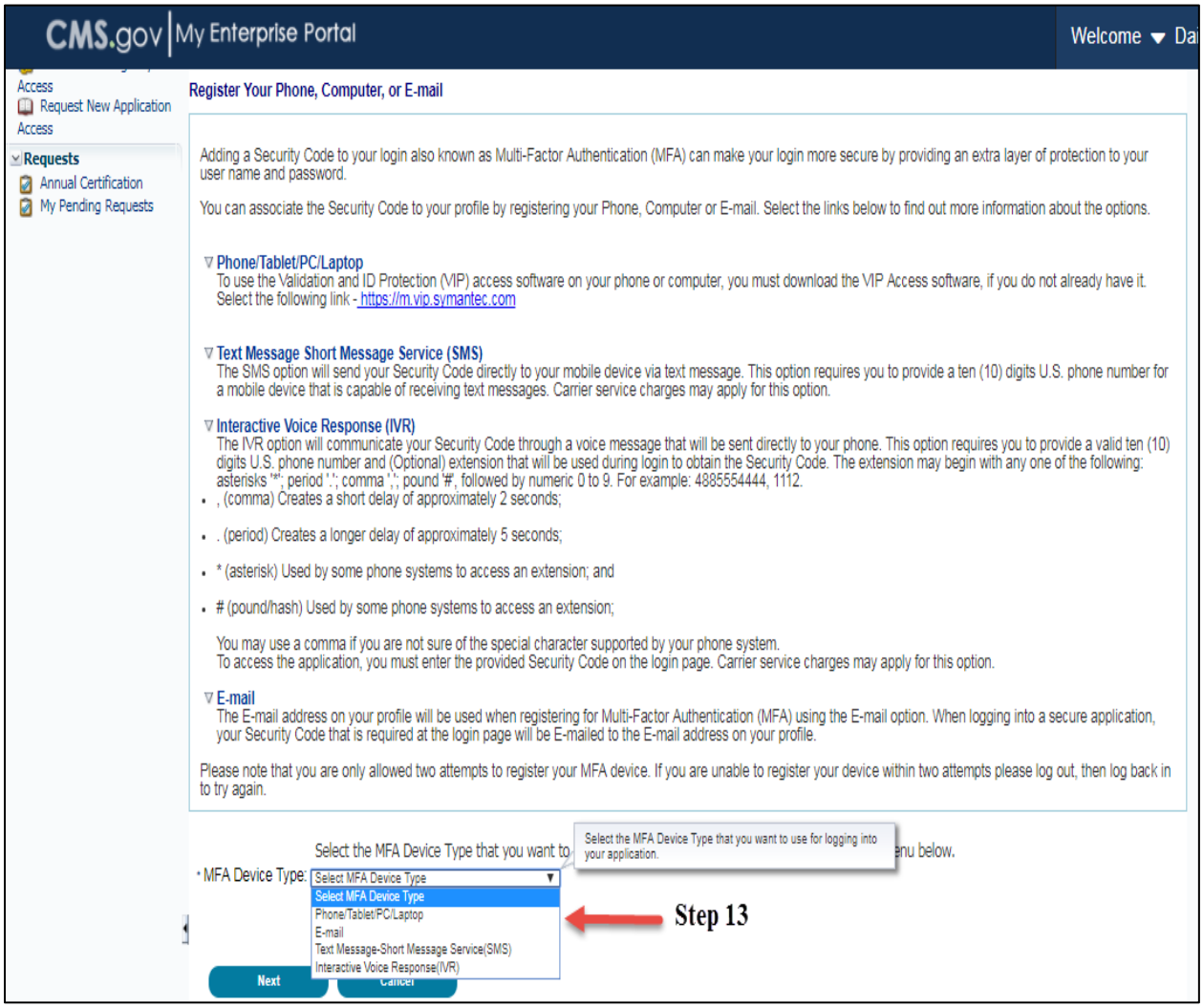


11. Remote Identity Proofing is now complete. Select '**Next**' to proceed to the '**Multi-Factor Authentication Registration**' process.



12. Select '**Next**' to begin registration for '**Multi-Factor Authentication Information**' process.

13. Read the **Register Your Phone, Computer, or E-mail** notification and then select an option from the '**Credential Type**' drop-down menu.



14. (a) If selecting **Phone/Tablet/PC/Laptop** as Credential Type, the following required information fields will be displayed: **NOTE:** If you intend to use the VIP access software on your mobile device or computer, you must download the VIP software.

    - Credential ID
    - Credential Description

    (b) f selecting **E-mail One Time Password** (OTP) as Credential Type, the following required information fields will be displayed:

    - E-mail
    - Credential Description

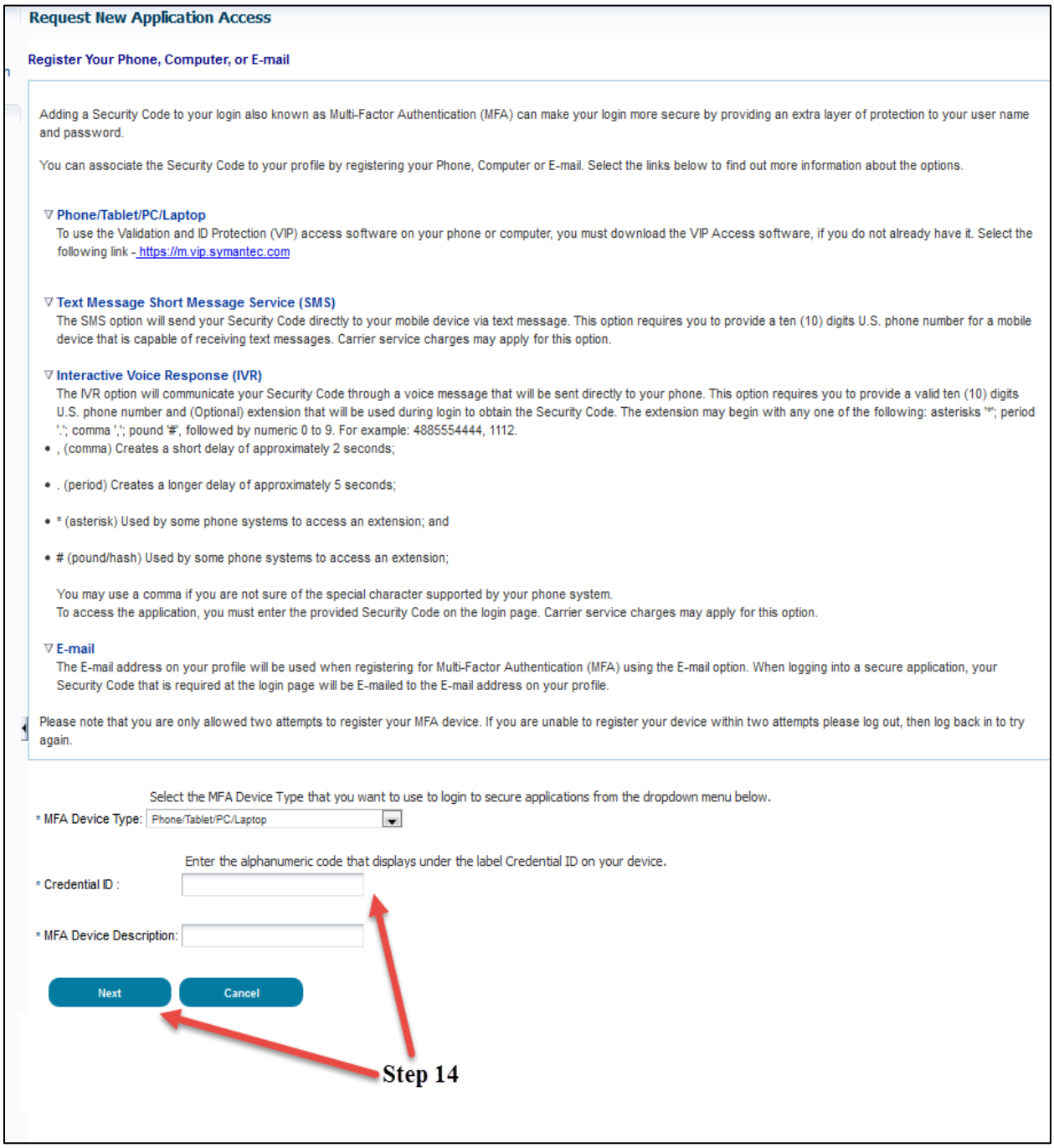
    (c) If selecting **Text Message – Short Message Service** (SMS) as Credential Type, the following required information fields will be displayed:

    - Phone Number
    - Credential Description

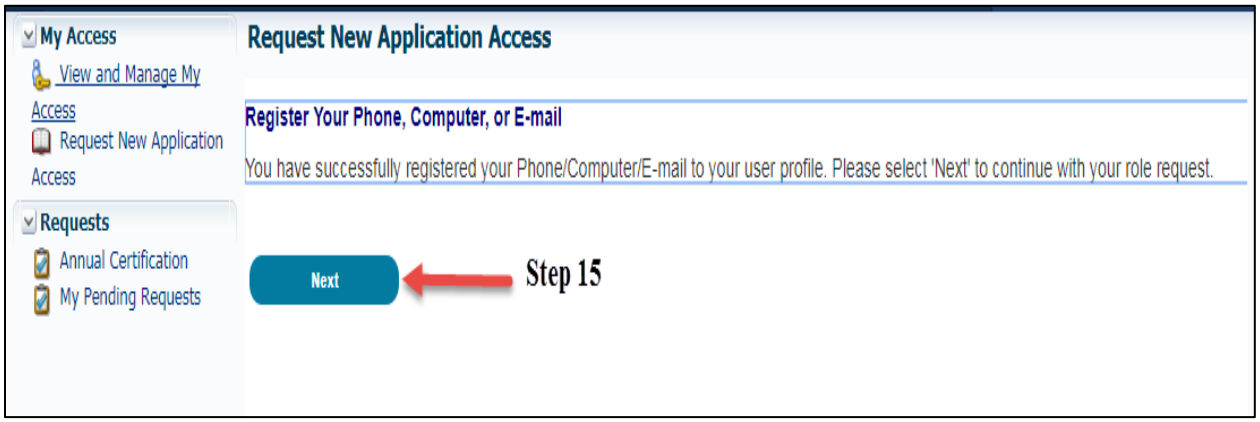
    (d) If selecting **Interactive Voice Response (IVR)** as Credential Type, the following required information fields will be displayed:

    - Phone Number
    - Credential Description

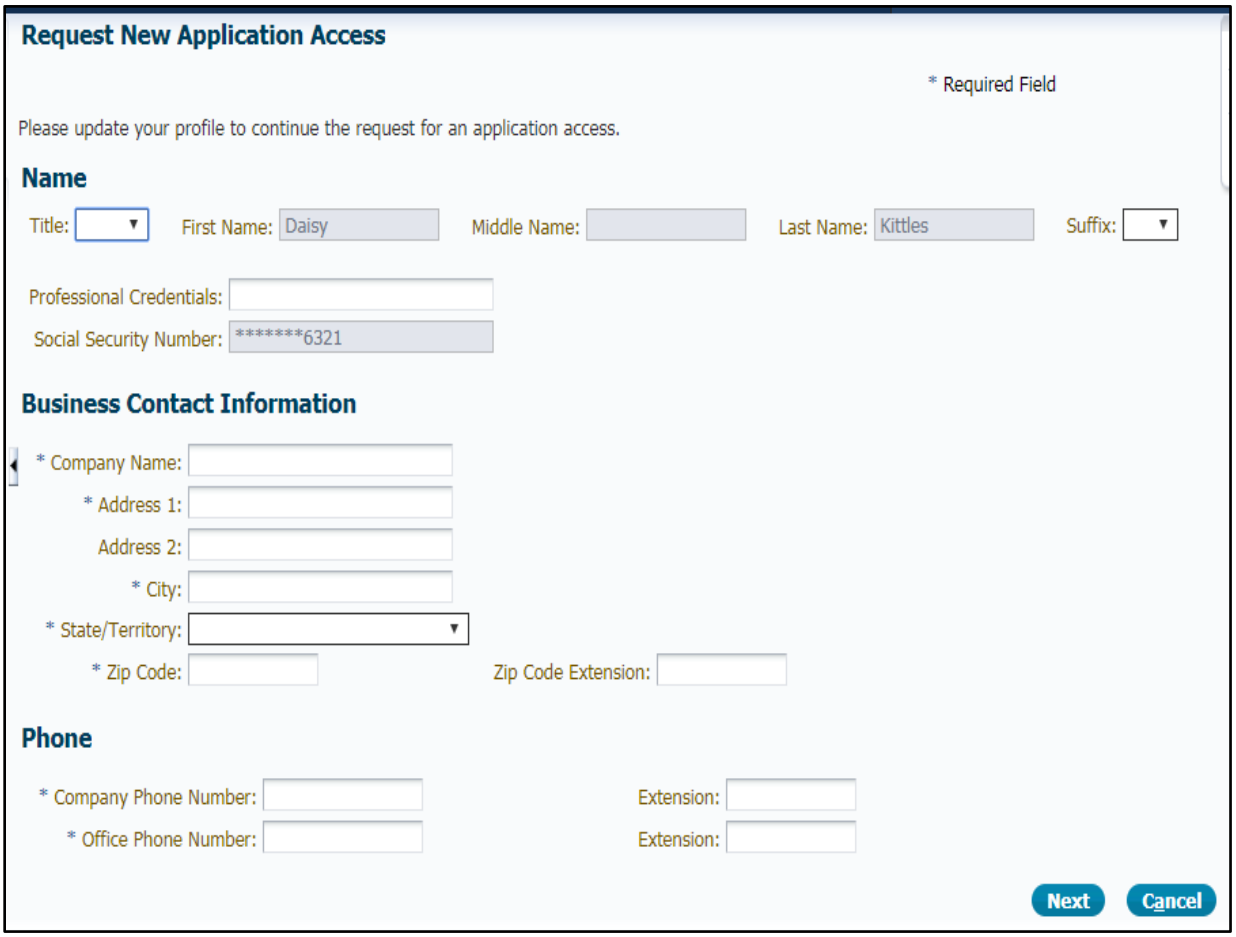
    After providing the required information, select '**Next**'.


Request New Application Access
Register Your Phone, Computer, or E-mail
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.
You can associate the Security Code to your profile by registering your Phone, Computer or E-mail. Select the links below to find out more information about the options.
Phone/Tablet/PC/Laptop
To use the Validation and ID Protection (VIP) access software on your phone or computer, you must download the VIP Access software, if you do not already have it. Select the following link - https://m.vip.symantec.com
Text Message Short Message Service (SMS)
The SMS option will send your Security Code directly to your mobile device via text message. This option requires you to provide a ten (10) digits U.S. phone number for a mobile device that is capable of receiving text messages. Carrier service charges may apply for this option.
Interactive Voice Response (IVR)
The IVR option will communicate your Security Code through a voice message that will be sent directly to your phone. This option requires you to provide a valid ten (10) digits U.S. phone number and (Optional) extension that will be used during login to obtain the Security Code. The extension may begin with any one of the following: asterisks '*'; period '.'; comma ','; pound '#', followed by numeric 0 to 9. For example: 4885554444, 1112.
• , (comma) Creates a short delay of approximately 2 seconds;
• . (period) Creates a longer delay of approximately 5 seconds;
• * (asterisk) Used by some phone systems to access an extension; and
• # (pound/hash) Used by some phone systems to access an extension;
You may use a comma if you are not sure of the special character supported by your phone system.
To access the application, you must enter the provided Security Code on the login page. Carrier service charges may apply for this option.
E-mail
The E-mail address on your profile will be used when registering for Multi-Factor Authentication (MFA) using the E-mail option. When logging into a secure application, your Security Code that is required at the login page will be E-mailed to the E-mail address on your profile.
Please note that you are only allowed two attempts to register your MFA device. If you are unable to register your device within two attempts please log out, then log back in to try again.
Select the MFA Device Type that you want to use to login to secure applications from the dropdown menu below.
* MFA Device Type: Phone/Tablet/PC/Laptop
Enter the alphanumeric code that displays under the label Credential ID on your device.
* Credential ID :
* MFA Device Description:
Next
Cancel
Step 14

15. Registration for the **Multi-Factor Authentication** is now complete. Select '**Next**' to proceed to request the role.



16. **MFA** is now complete and **Business Contact Information** screen is displayed. Enter the required information under **Business Contact Information** and **Phone** section and Select Next.

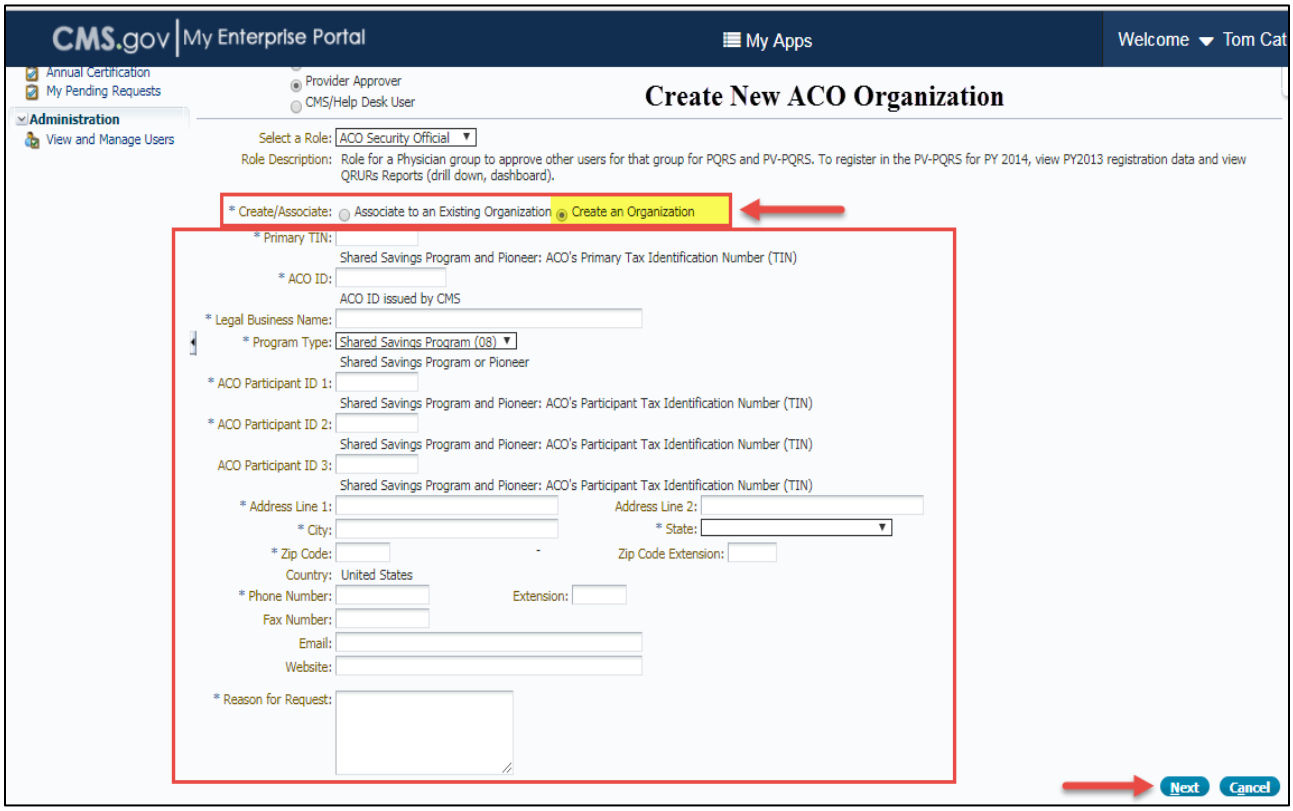


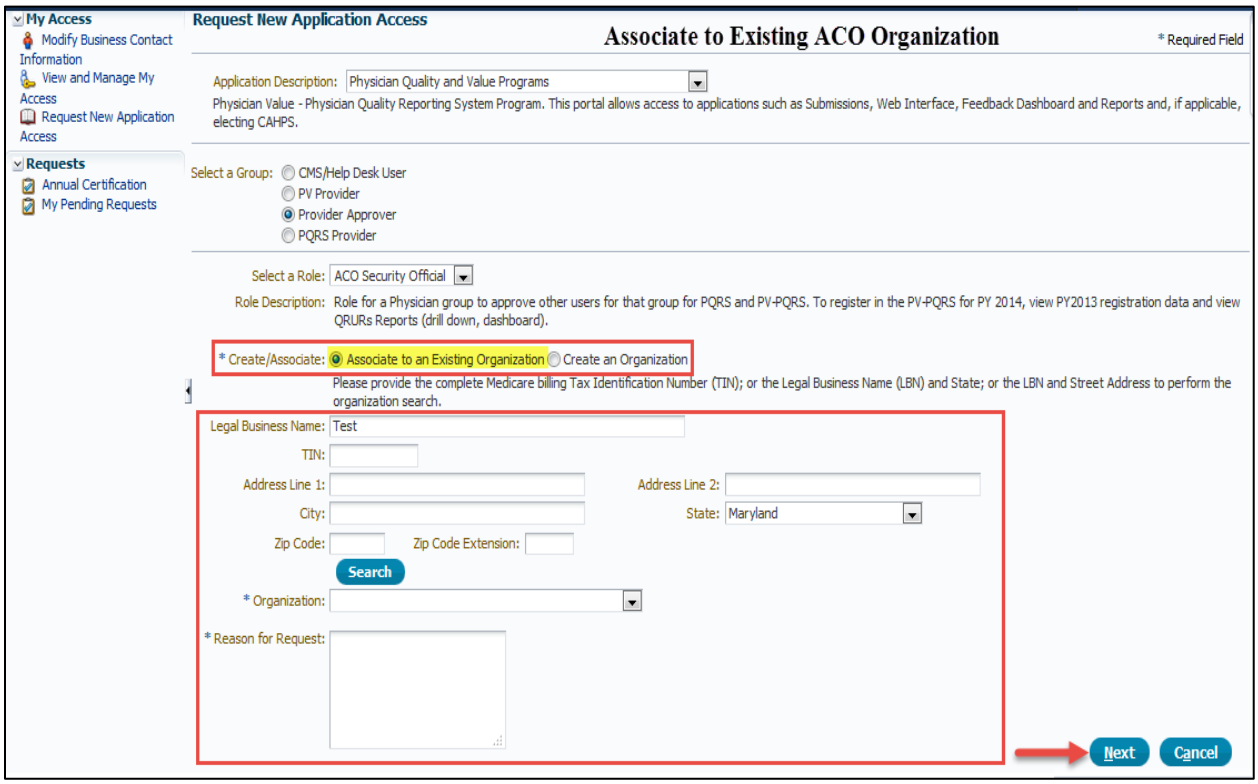
17. To create your ACO Security Official:

- Select '**Create an Organization**' (screen shot '**Create New ACO Organization**' on page 21) if you are registering your first ACO Security Official on behalf of your ACO.
- If your ACO has already set up the first ACO Security Official role and would like to request additional ACO Security Officials, then please select '**Associate to an Existing Organization**' (screen shot 'Associate to Existing ACO Organization' on page 22).
- Complete the required information for '**Create an Organization**' or enter the search criteria and select the appropriate organization for '**Associate to an Existing Organization**'. Once the form has been completed, including entering a '**Reason for Request**', select '**Next'.**

NOTE: You must use the Primary (ACO) TIN, the CMS ACO ID, and at least 2 participant TINs for setting up your ACO Security Official role.

Single TIN Shared Savings Program ACOs: If your ACO is a single TIN ACO, then due to limited data available, your ACO must be routed to the QPP Service Center for manual approval. Your ACO SO submission will be routed to the QPP Service Center and you will receive a tracking number. Updates to your role request status will be provided via email. For support and questions, the QPP Service Center can be reached at 1-866-288-8292 or qpp@cms.hhs.gov (Business hours are Monday-Friday from 7am to 7pm Central Time).



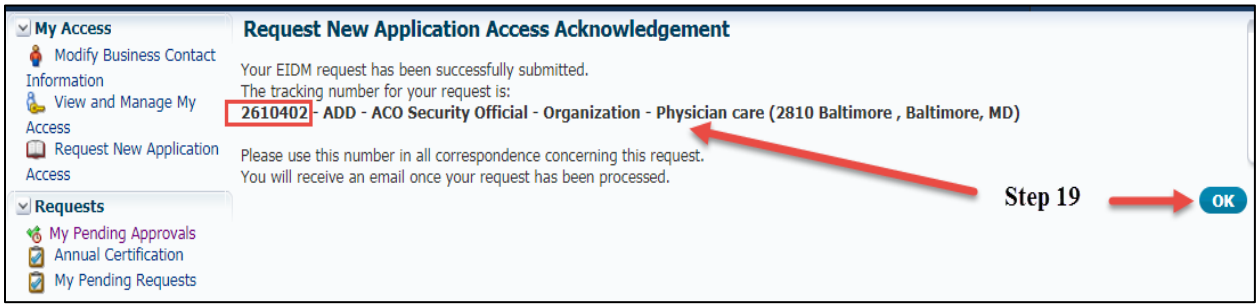


NOTE: Make sure that the search criteria entered is accurate. If the organization is unable to be found, contact the QualityNet Help Desk for assistance.

When associating to an existing organization, the request will be sent to the ACO Security Official for approval. ACO SOs creating an organization who are participating in the Shared Savings Program be approved in the system without being routed to the QualityNet Help Desk, if all data entry matches CMS records and your ACO is not a single-TIN ACO.

18. Review the entire request to confirm all of the data was entered accurately. If the information is accurate, select **'Submit'**. If a change needs to be made, select **'Edit'** and make the appropriate changes.

19. A tracking number will be displayed on screen, select **'ok'.** The tracking number is also sent via email to the requestor. This tracking number should be retained until the requested role has been applied to the account.



NOTES: The ACO SO who created the organization is the approver for subsequent ACO SOs associating to the organization.

- The approver (ACO SO) will receive an email notifying them of the request for an ACO SO associating to the organization for approval.
- The approver (ACO SO) will need to log into the CMS Enterprise Portal to approve or reject the request.

  The notification of approval, denial, or other requests will be sent to the role requestor's email address on file for the request.

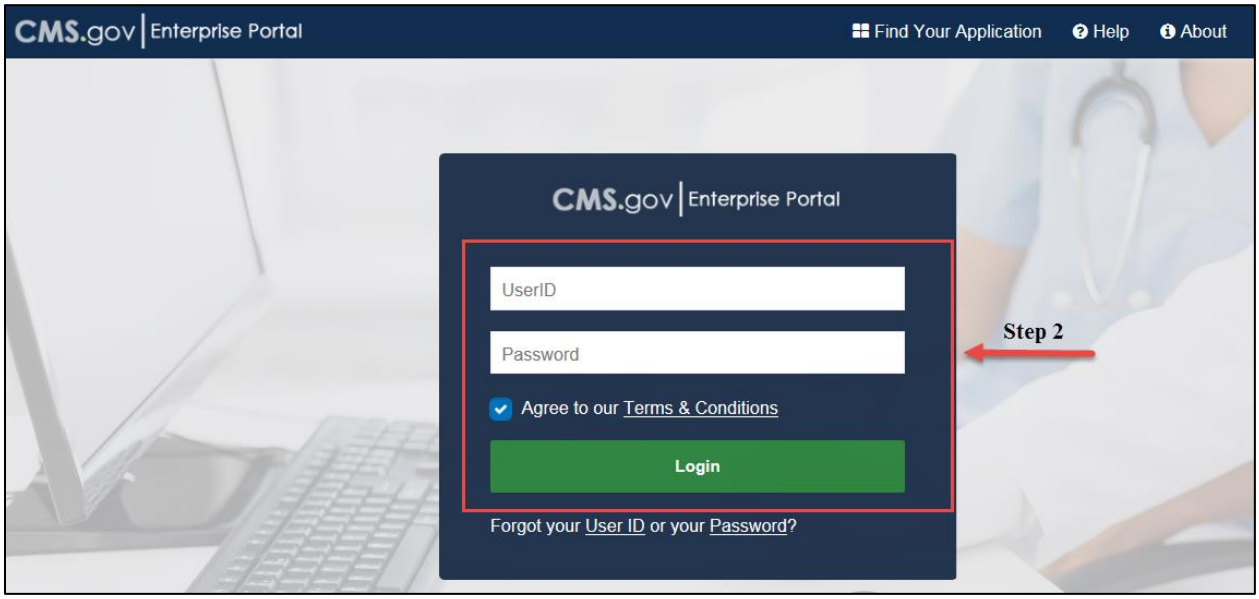
How to Set Up the Web Interface Submitter Role

After an ACO SO role has been created and approved, a Web Interface Submitter Role must be established. The Web Interface Role cannot be set up until there is at least one ACO SO role set up.

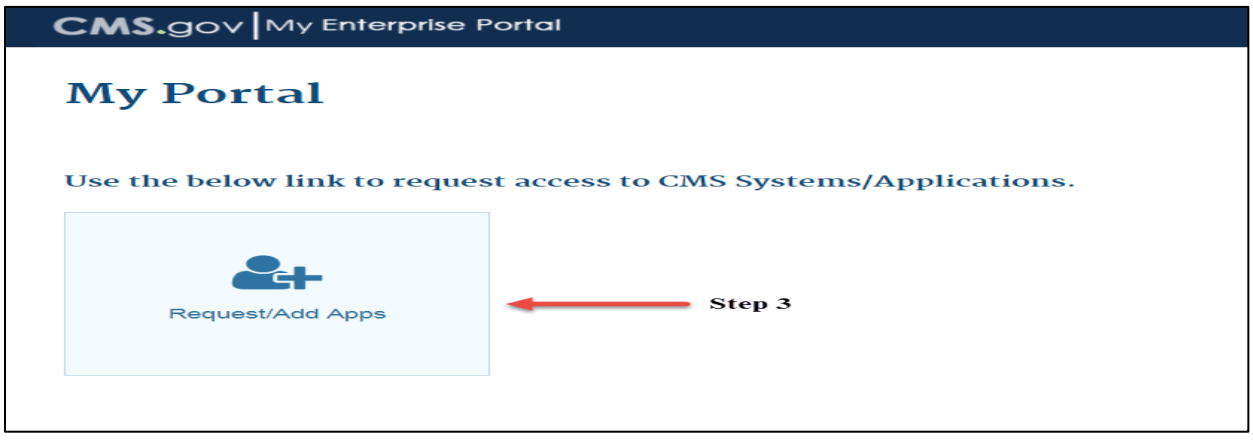
Steps to Create a Web Interface Submitter Role:

1. Navigate to https://portal.cms.gov. The CMS Enterprise Portal page is displayed.

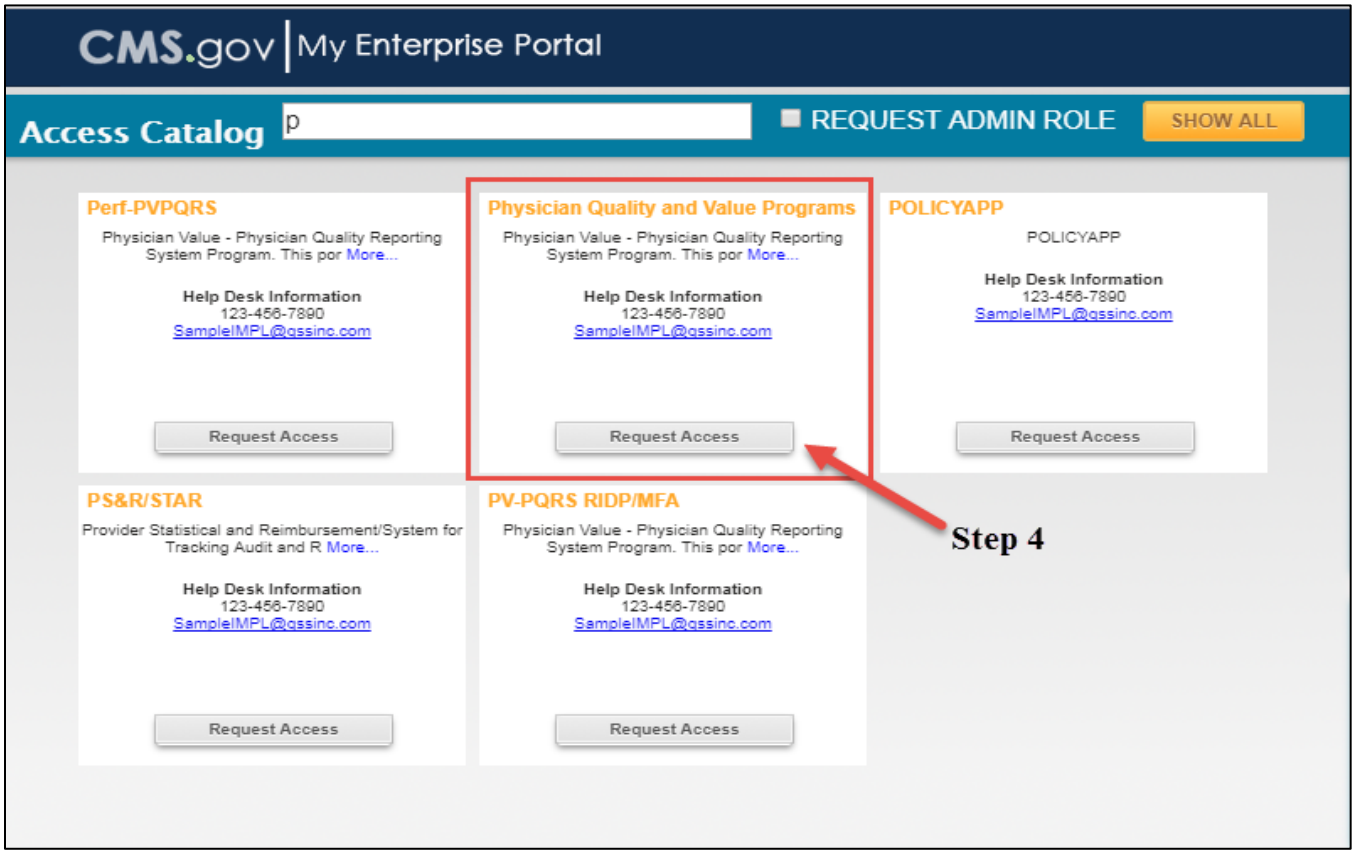
2. Once on the page, enter your user ID and password and agree to Terms and Conditions by clicking the checkbox.



3. The **'My Portal'** page is displayed. Select the **'Request/Add Apps'** link to request access to CMS Systems/Applications.



4. For the PQRS and the PV-PQRS Applications; scroll down and select **'Request Access'** for the **'Physician Quality and Value Programs'** application.

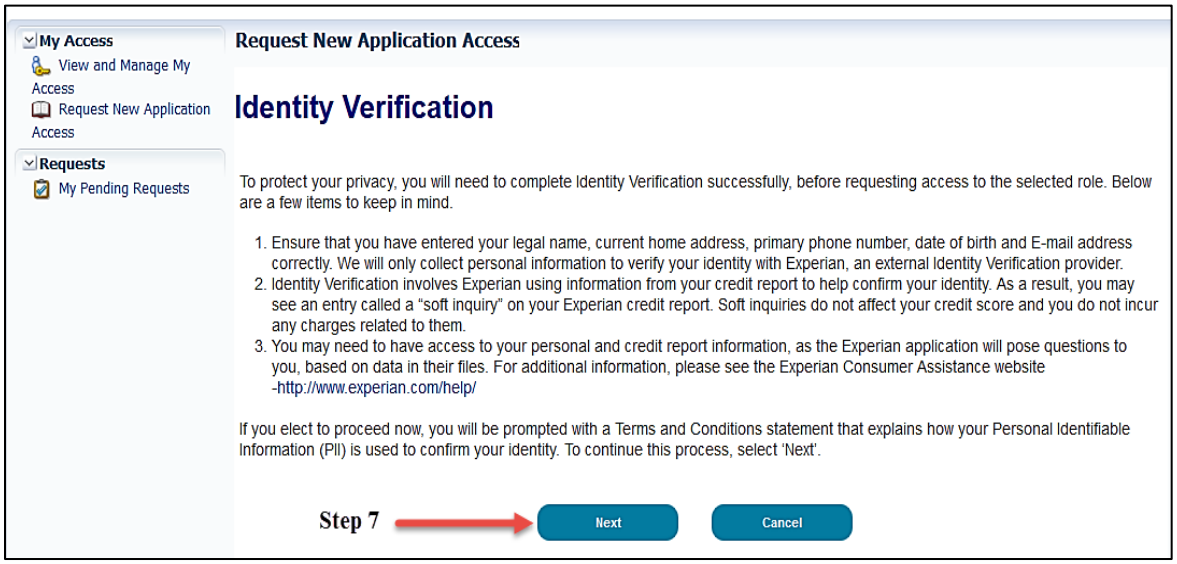


5. The Physician Quality and Value Programs Domain will be auto-populated. Under '**Select a Group**', select '**PQRS Provider**.'

6. Select '**Web Interface Submitter**' under '**Select a Role**' from the drop-down menu.

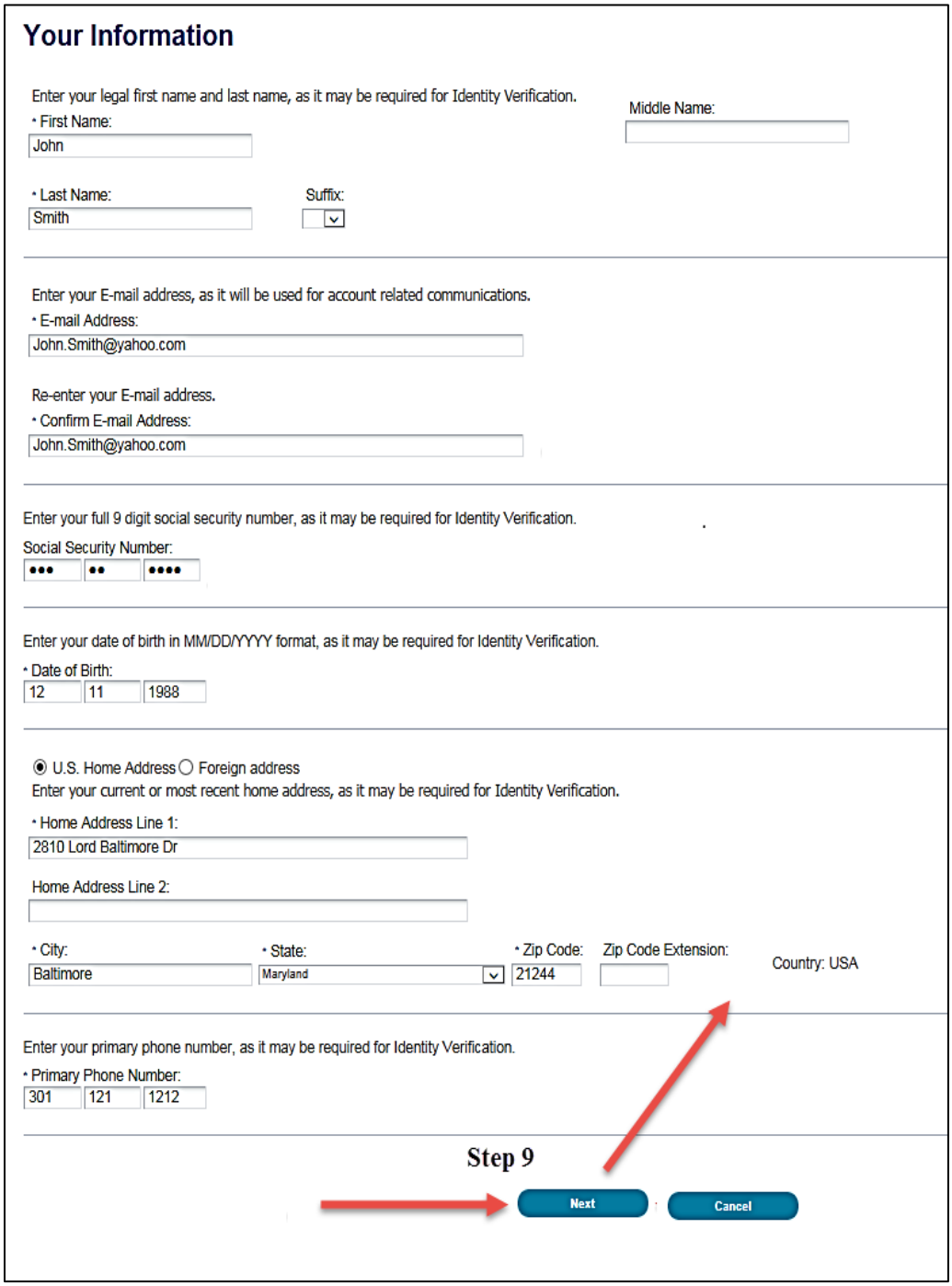
7. Select '**Next**' to complete the '**Identity Verification**' section. The Identity Verification process will only be completed the first time a user requests a role in the Physician Quality and Value Programs domain in EIDM. If the Identity Verification has been completed, users can skip to step 17 to request additional roles.

   NOTE: Users must be in the United States of America to complete Identity Verification.

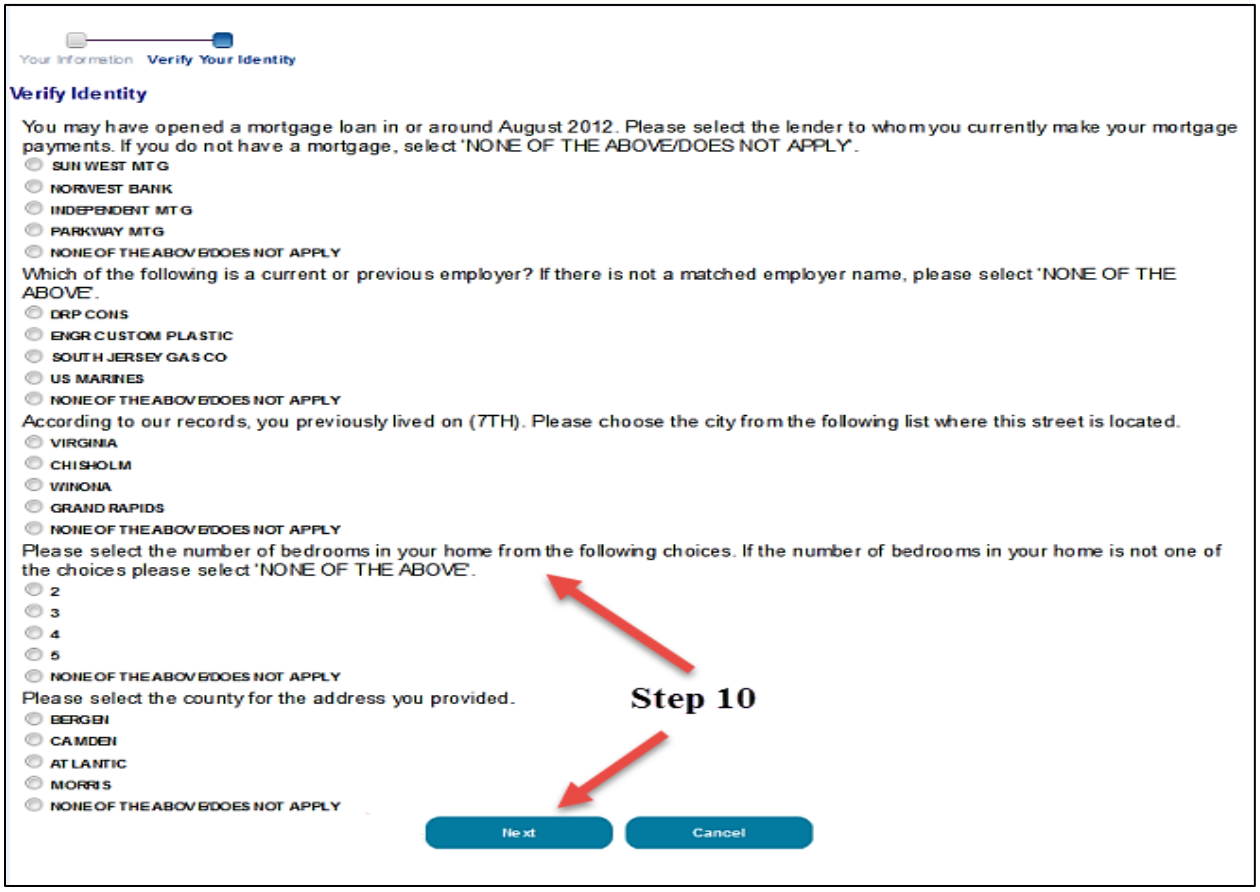


8. Read the Terms and Conditions. Select the '**I agree to the terms and conditions**' checkbox and then select '**Next**'. '**Next**' will be enabled only after checking the '**I agree to the terms and conditions**' checkbox

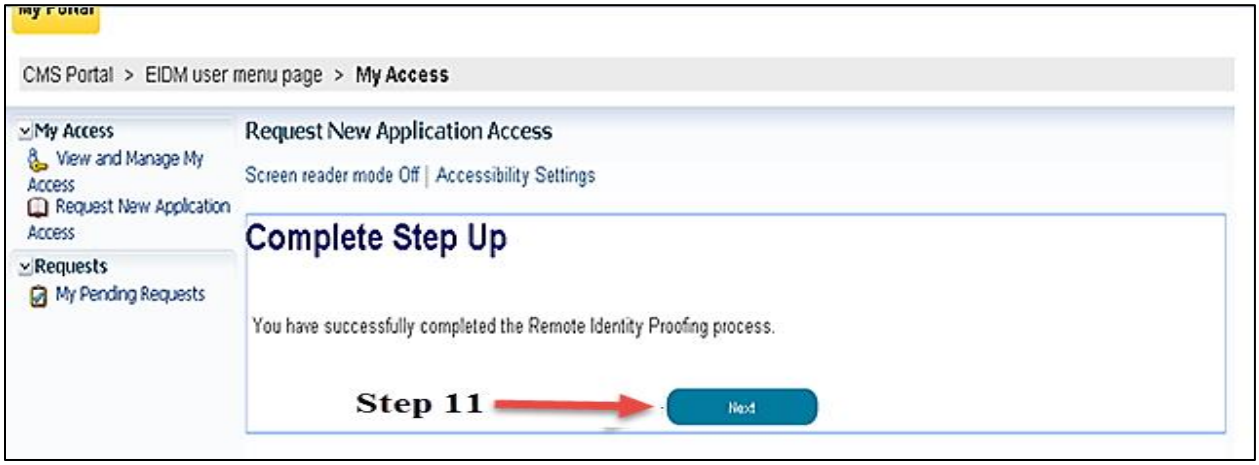
9. Enter the required information under Your Information section. Select '**Next**' when complete.



10. Select an answer to each question under '**Verify Identity**'. Select '**Next**' after providing an answer to each question. '**Verify Identity**' question information is provided from Experian in association with the SSN provided in step 9.

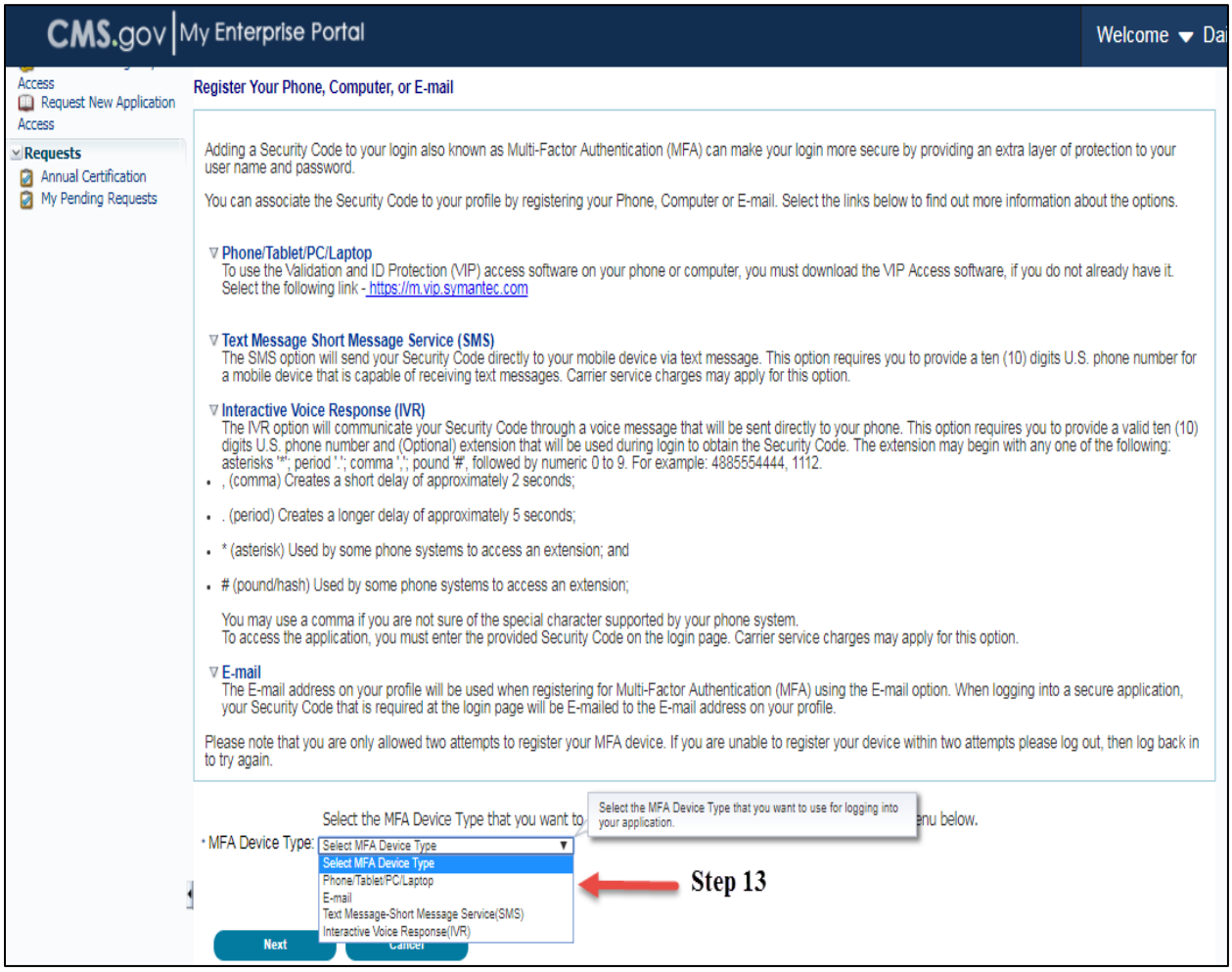


11. Remote Identity Proofing is now complete. Select '**Next**' to proceed to the '**Multi-Factor Authentication Registration**' process.



12. Select '**Next**' to begin registration for '**Multi-Factor Authentication Information**' process.

13. Read the **Register Your Phone, Computer, or E-mail** notification and then select an option from the '**Credential Type**' drop-down menu.



14. (a) If selecting **Phone/Tablet/PC/Laptop** as Credential Type, the following required information fields will be displayed:

    - Credential ID
    - Credential Description

    (b) If selecting **E-mail One Time Password (OTP)** as Credential Type, the following required information fields will be displayed:

    - E-mail
    - Credential Description

    (c) If selecting **Text Message** – **Short Message Service (SMS)** as Credential Type, the following required information fields will be displayed:

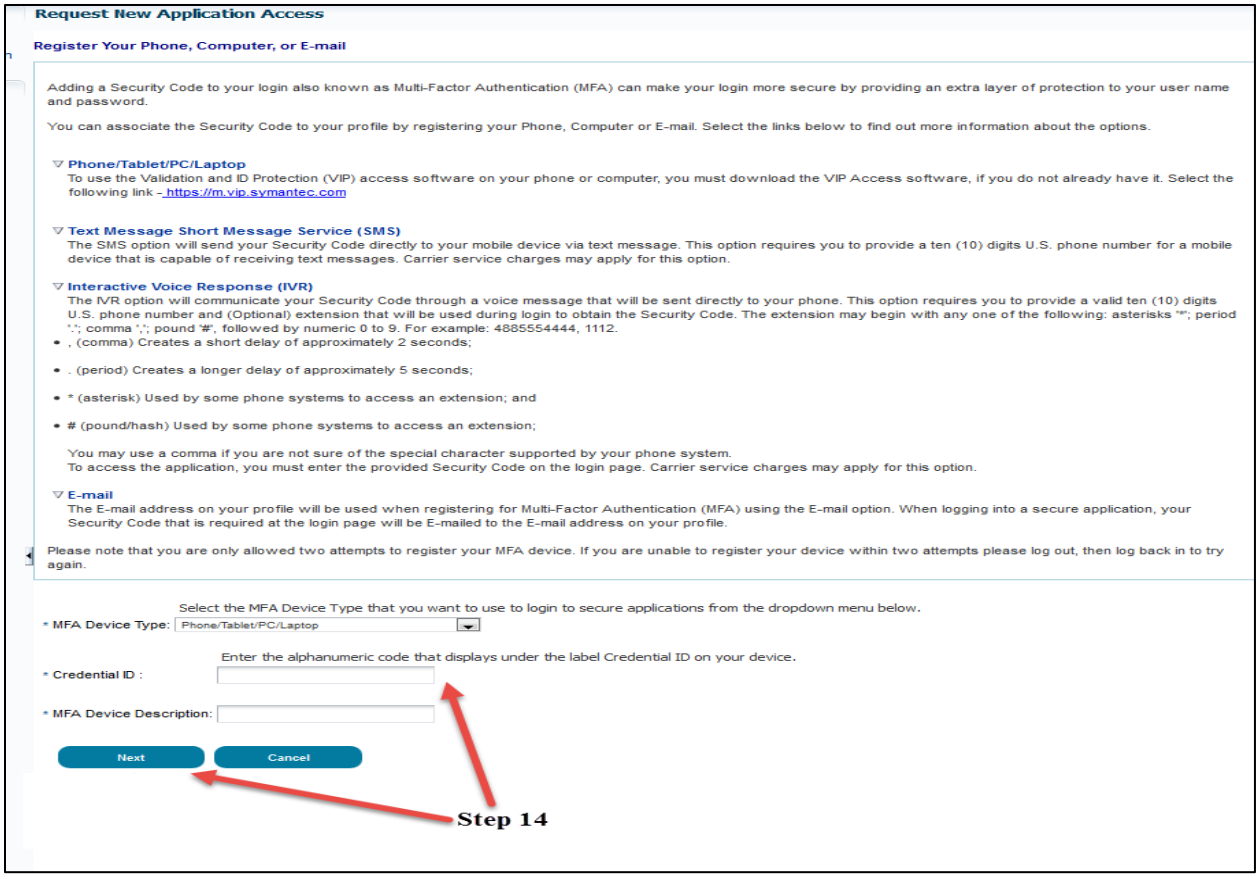
    - Phone Number
    - Credential Description

    (d) If selecting **Interactive Voice Response (IVR)** as Credential Type, the following required information fields will be displayed:

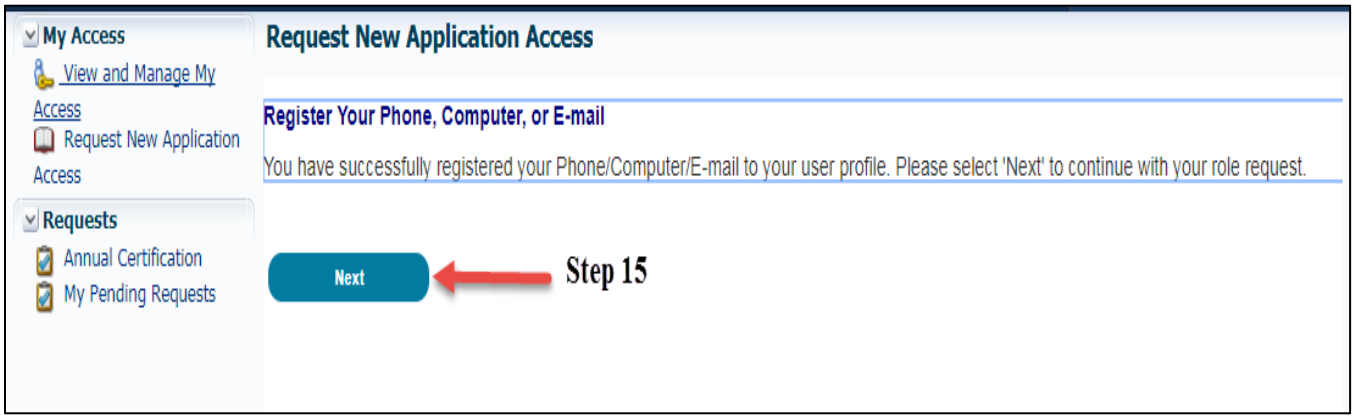
    - Phone Number
    - Credential Description

    NOTE: If you intend to use the VIP access software on your mobile device or computer, you must download the VIP software.

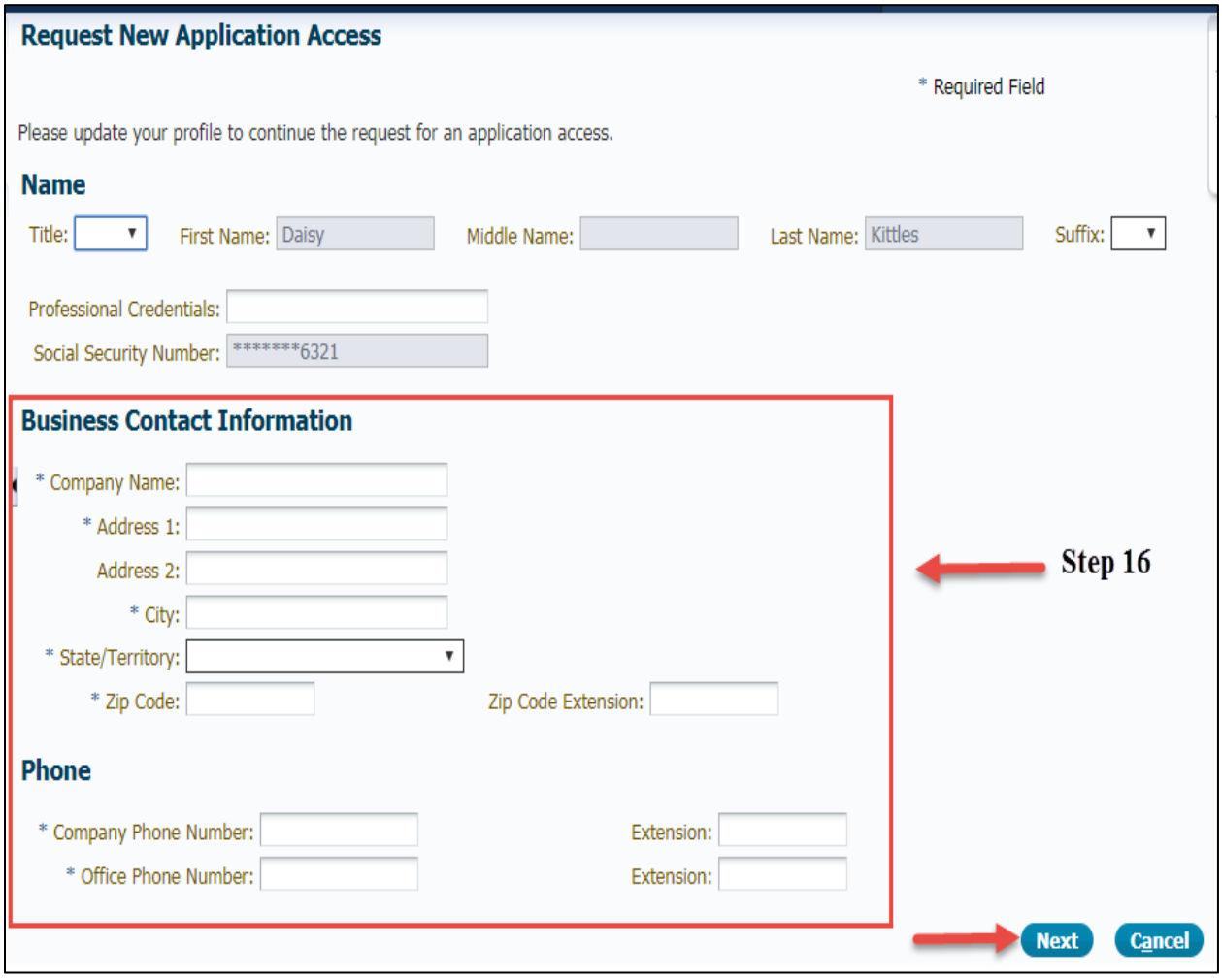
    After providing the required information, select '**Next**'.



15. Registration for the **Multi-Factor Authentication** is now complete. Select '**Next**' to proceed to request the role.

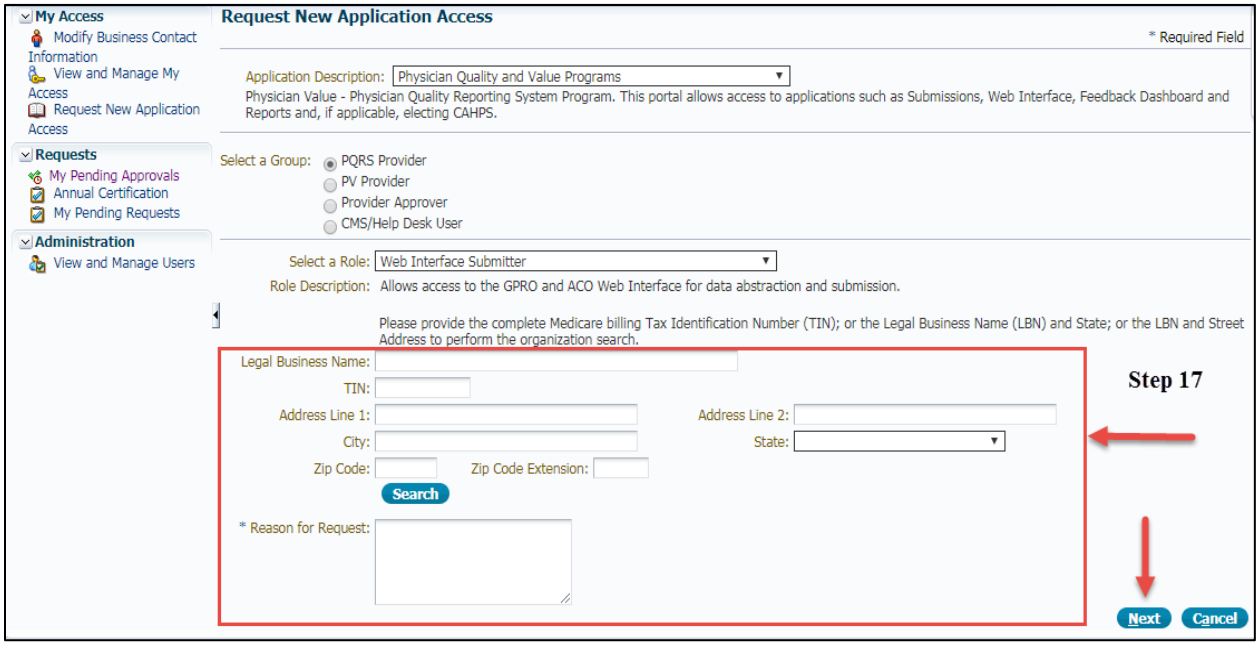


16. Enter required **Business Contact Information**. Once the required information has been entered, select '**Next**' to continue.



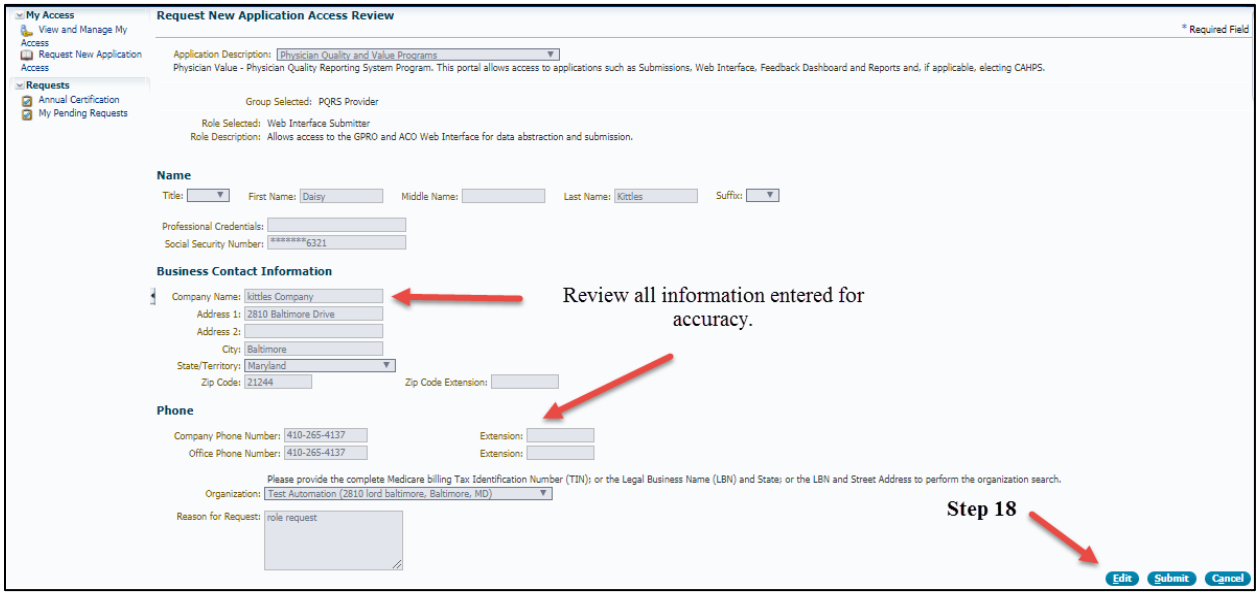
17. Enter the specific criteria to search the existing Organization and select '**Search**'. When the desired Organization has been found, associate to it and enter a '**Reason for Request**' then select '**Next**'.

    NOTE: Please use the ACO Primary TIN when completing the TIN field.

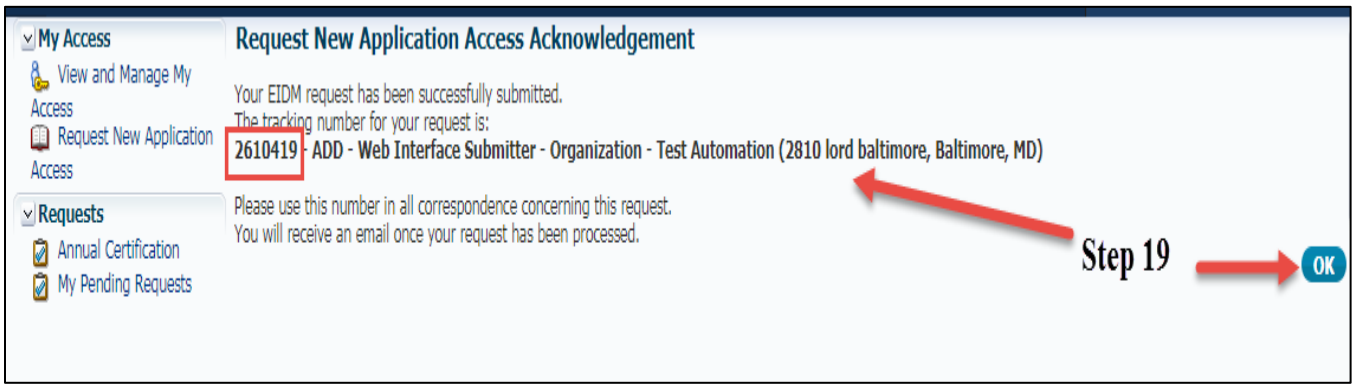


18. Review the request to confirm the accuracy of the role request and organization affiliation. Select '**Submit**' to complete the request or '**Edit**' to make any corrections.

    NOTE: Information was removed from this screen shot but the user will see all required information entered.



19. Role request acknowledgement provides the tracking number that will also be sent via email to the requestor. Select '**OK**. This tracking number should be retained until the requested role has been applied to the account.



NOTES:

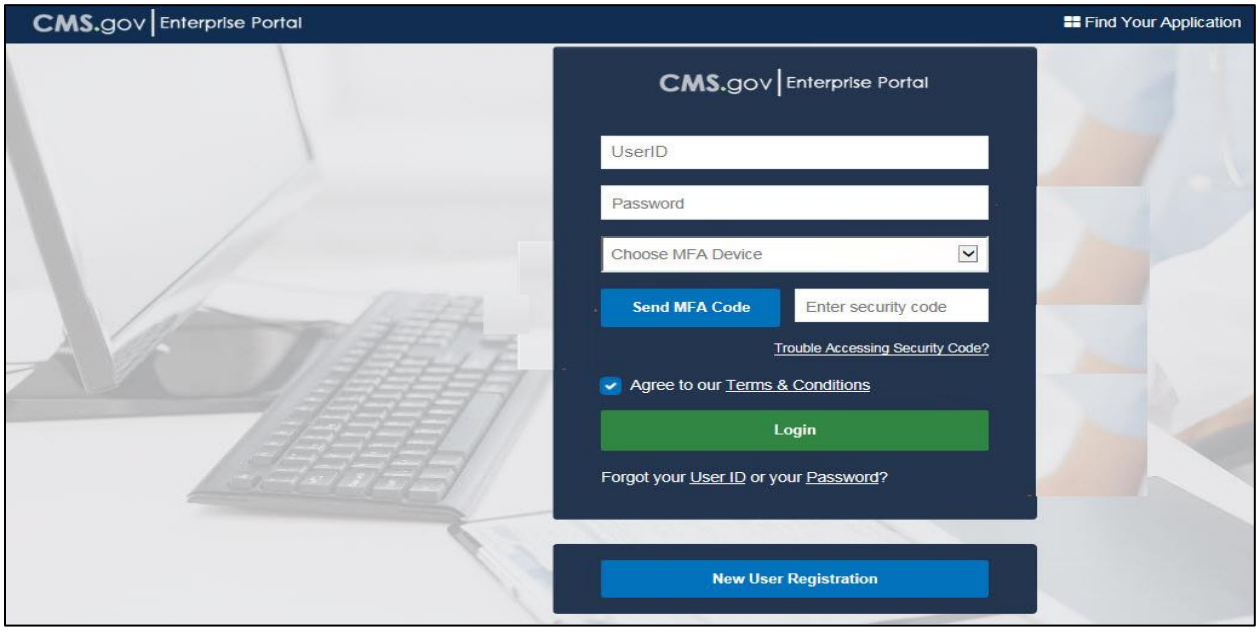
- The above role requests will be directed to the appropriate approver(s), which are the ACO SOs, for the organization to complete the process.
- The approver(s) will receive an email notifying them of the request for approval.
- The approver will need to log into the CMS Enterprise Portal to approve or reject the request.

  The notification of approval, denial, or other requests will be sent to the role requestor's email address on file for the request.

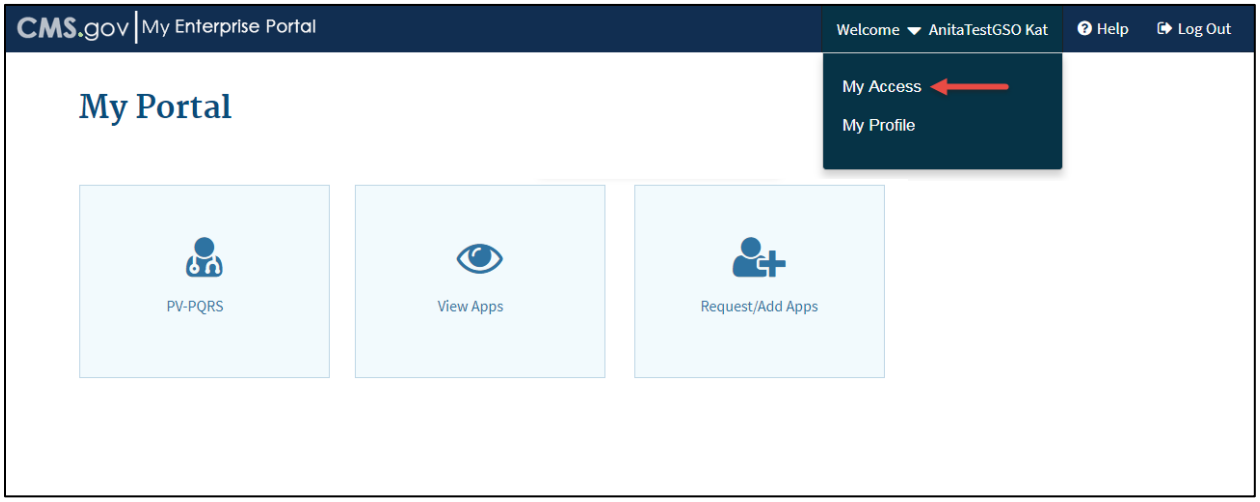
How to Check Your Role Status

Users can check their approved EIDM roles by logging into the CMS Enterprise Portal using their EIDM account and following the steps outlined below. Please note screenshots are taken from a test environment and may not display exactly what you see on your screen.

1. Login to CMS Enterprise Portal using valid EIDM user ID and password and completing MFA process. As a reminder, this is **not** the CMS user ID (EUA) that is used for accessing the Shared Savings Program ACO portal or HPMS. You must use your EIDM user ID.



2. After successfully logging into the CMS Enterprise Portal using your EIDM user ID, password, and completing MFA process, **click on Welcome <Your Name>** at the top right of your screen. Once selected, a dropdown will allow you to then **click on My Access**.

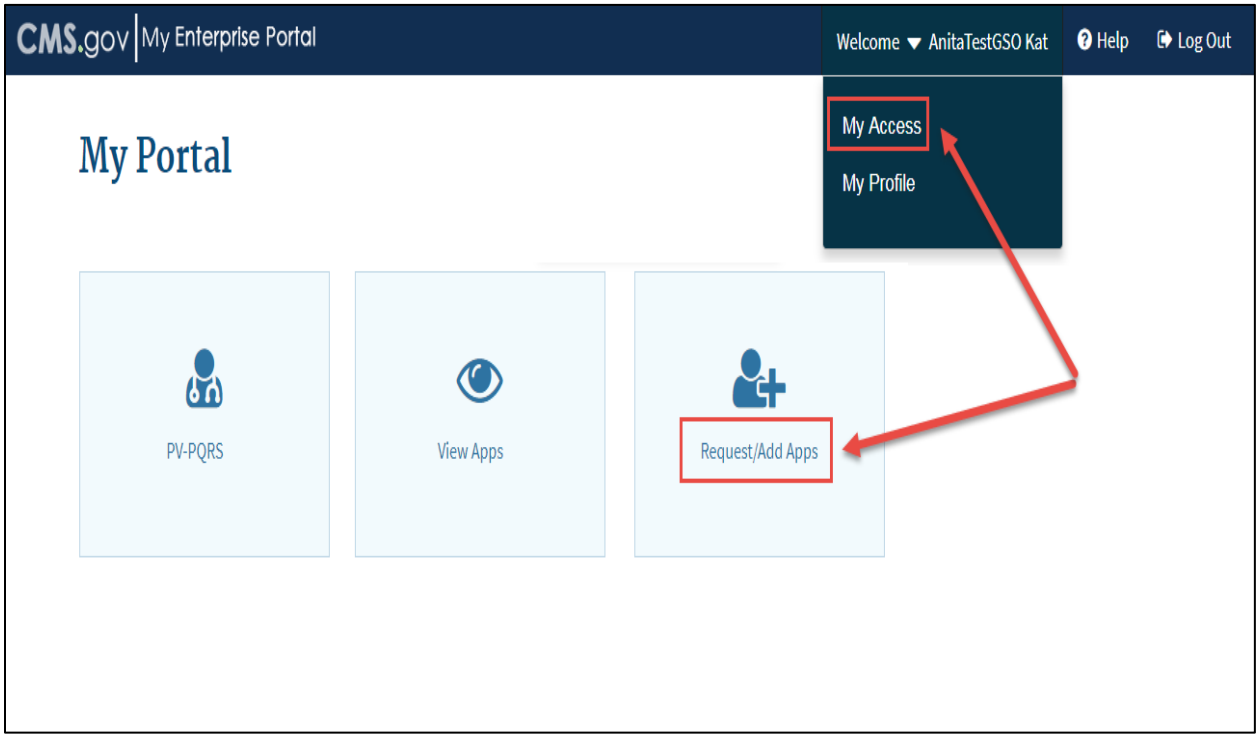


3. After selecting My Access, you will be able to view your approved roles. You may also take other actions, such as removing or adding another role. Please note, no single user can be both an ACO Security Official and a Web Interface Submitter.

How to Remove a Role

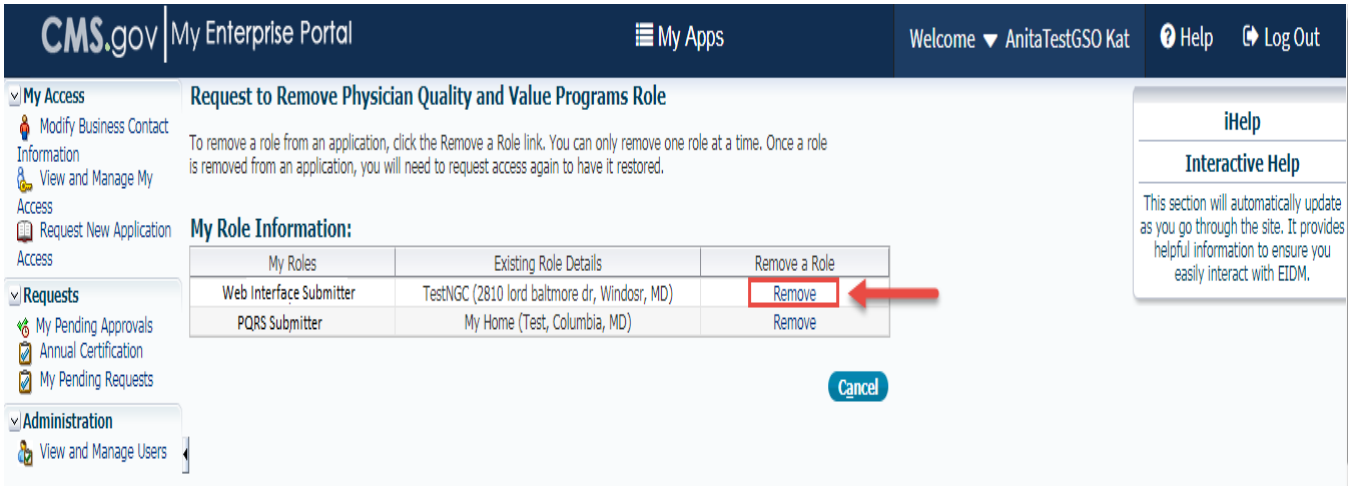
1. Login to CMS Enterprise Portal using your valid EIDM user ID and password.

2. Select one of two options:
   - Click on **Welcome <your name>** at the top right corner of the form. Once selected **click on My Access** value in the dropdown.
     OR
   - Click on **Request/Adds Apps** option.

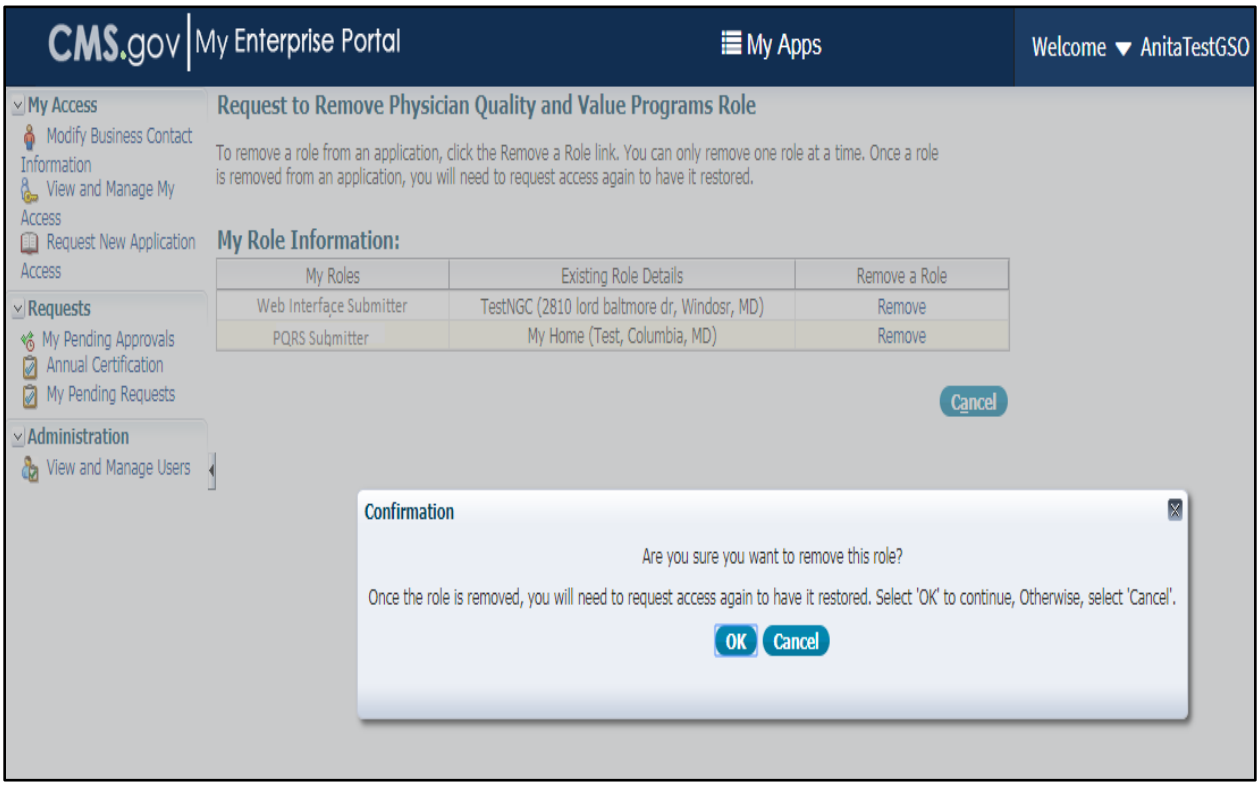


3. The **Available Actions** menu will be displayed on your screen. Click on the **Remove Role** option.

4. The screen will display you user roles. Click on the **Remove** hyperlink that is next to the role you want to remove from your profile.



5. A **Confirmation** pop-up will be displayed. Click on **OK** to confirm role removal. After clicking ok, a confirmation of role removal will be displayed.



Technical Assistance

If you have questions or need further assistance, please contact the QPP Service Center:

- QPP@cms.hhs.gov
- 1-866-288-8292

Business hours are Monday-Friday from 7am to 7pm Central Time.