

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





Table of Contents

Topic	Page Number
Introduction	3
EIDM Accounts and Roles Overview	3
How to Register and Create EIDM Accounts	6
How to Set Up ACO Security Official (SO) Role.....	12
How to Set Up the Web Interface Submitter Role.....	25
How to Check Your Role Status	39
How to Remove a Role	41
Technical Assistance	44

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) and access its Merit-based Incentive Payment System (MIPS) performance feedback. When available, the CMS WI and MIPS performance feedback will be accessible through the Quality Payment Program (QPP) Portal that will be available on the QPP website at qpp.cms.gov and announced through the ACO Spotlight Newsletter.

This ACO guide describes EIDM roles for the ACO Security Official and the ACO's Web Interface Submitter only.

EIDM accounts will allow your ACO to:

- Access the QPP Portal qpp.cms.gov;
- Access the CMS WI to download your Beneficiary Sample prior to the CMS WI data submission period;
- Access the CMS WI training environment;
- Enter and submit quality data via the CMS WI during the submission period to fulfill program requirements for complete and accurate reporting.
- Access the ACO's MIPS performance feedback and payment adjustment information; and
- Submit a targeted review request on qpp.cms.gov

Groups and individual practitioners participating in an ACO should refer to the [MIPS EIDM User Guide](#) for guidance on creating group or individual EIDM roles.

EIDM Accounts and Roles Overview

In order to report CMS WI data and access its MIPS performance feedback, 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 and to access MIPS performance feedback.

Role	Responsibilities	Approval
<p>ACO Security Official (ACO SO)</p>	<p>User must be from the ACO and approves Web Interface Submitter role requests by EIDM account holders for their organization. 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. The ACO SO can also access the ACO's MIPS performance feedback and payment adjustment information, and submit a targeted review request on qpp.cms.gov.</p> <p>*All users must be in the United States of America.</p>	<p>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 QPP Service Center for manual approval. Please contact the QPP Service Center at qpp@cms.hhs.gov for assistance.</p> <p>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.</p>

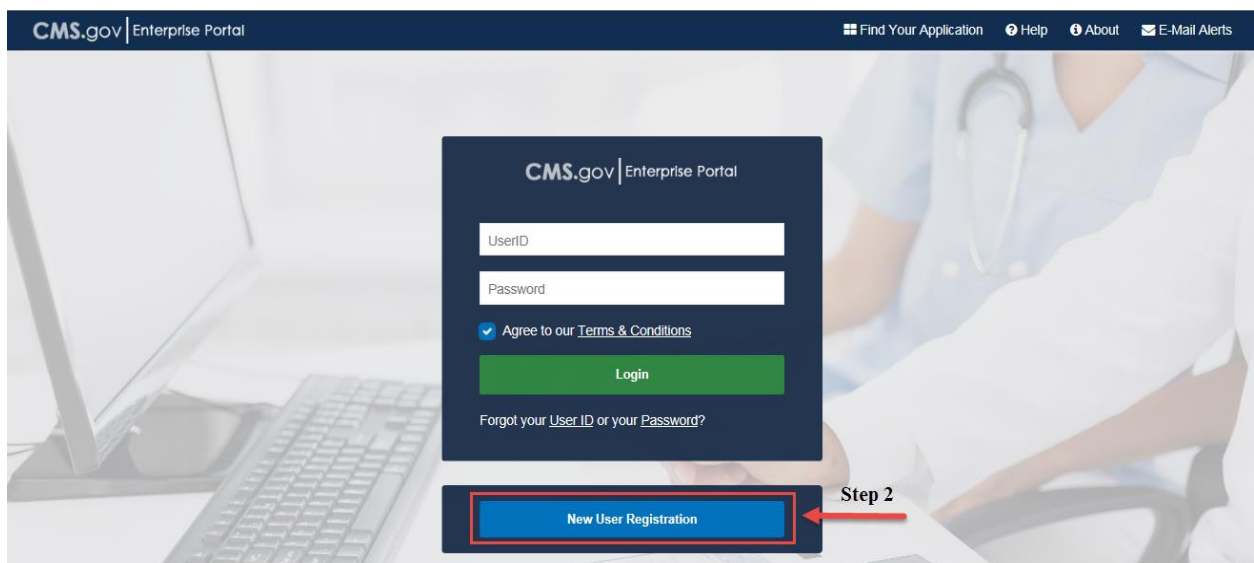
Role	Responsibilities	Approval
Web Interface Submitter	<p>User has access to the CMS WI, through the QPP Portal, to download the Beneficiary Sample, participate in the training environment, enter and submit quality data, and generate reports. The Web Interface submitter can also access the ACO's MIPS performance feedback and payment adjustment information, and submit a targeted review request on qpp.cms.gov.</p> <p>Note: An organization must have an ACO Security Official before a user can request the Web Interface Submitter role.</p> <p>To determine the ACO's Security Official, please contact the QPP Service Center at 1-866-288-8292 / TTY 877-715-6222 or by email at qpp@cms.hhs.gov. You will need to provide the ACO's Primary TIN and Legal Business Name.</p> <p>*Third party vendors may be a Web Interface Submitter, but all users must be in the United States of America.</p>	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.

CMS.gov | Enterprise Portal Find Your Application Help Ab

Step #1: Choose Your Application

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

Choose Your Application ▼

- PQRS: Physician Quality Reporting System
- PSR/STAR: Provider Statistical and Reimbursement/System for Tracking Audit and Reimbursement
- PV: Physician Quality and Value Programs** ← **Step 3**
- QARM: Quality Net Authorization & Role Management
- RNSGUI: Research and Support Graphical User Interface
- Salesforce: Salesforce/CMMI
- SERTS/SERVIS/CPMS: State Exchange Resource Virtual Information System/CO-OP Program Management System
- SHIM: Enrollment and Payment Portal
- SPOT(FCSO): First Coast Service Options Internet Portal
- STARS: Services Tracking Analysis and Reporting System
- T-MSIS: Transformed Medicaid Statistical Information System
- UCM: Unified Case Management
- VMS Client Letter: VMS Durable Medical Equipment DME Client Letter Application

- 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.

CMS.gov | Enterprise Portal Find Your Application

Step #2: Register Your Information

Step 2 of 3 - Please enter your personal and contact information.
All fields are required unless marked 'Optional'.

Enter First Name	Enter Middle Name (optional)	Enter Last Name	Suffix (optional) ▼
Enter Social Security Number (optional)	Birth Month ▼	Birth Date ▼	Birth Year ▼

Is Your Address US Based?

Yes No

Enter Home Address #1	Enter Home Address #2 (optional)		
Enter City	State ▼	Enter Zip Code	Enter Zip+4 (optional)
Enter E-mail Address	Confirm E-mail Address		
Enter Phone Number			

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.
- **Note:** Do not use the @ symbol when creating your User ID.
- **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.

Step #3: Create User ID, Password & Security

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

The screenshot shows a form with several sections. A red box highlights the 'Enter User ID' field, with a red arrow pointing to it from the label 'Step 5'. Another red box highlights the 'Enter Password' and 'Enter Confirm Password' fields, with a red arrow pointing to it from the label 'Step 6'. A third red box highlights the 'Select Security Question #1', 'Select Security Question #2', and 'Select Security Question #3' sections, with a red arrow pointing to it from the label 'Step 7'. At the bottom, a red arrow points to the 'Next' button, with the label 'Step 8' next to it. The 'Back' button is on the left, and the 'Cancel' button is on the right.

Enter User ID	Step 5		
Enter Password	Enter Confirm Password	Step 6	
Select Security Question #1	Enter Security Question #1 Answer	Step 7	
Select Security Question #2	Enter Security Question #2 Answer		
Select Security Question #3	Enter Security Question #3 Answer		
Back	Next	Cancel	Step 8

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.

Registration Summary

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

PQRS: Physician Quality Reporting System

All fields are required unless marked 'Optional'.

First Name: Daisy
Enter Middle Name (optional)
Last Name: Kittles
Suffix (optional)

Social Security Number (optional): 258456321
Birth Month: January
Birth Date: 1
Birth Year: 1982

Home Address #1: 2810 Baltimore
Enter Home Address #2 (optional)

City: Baltimore
State: Maryland
Zip Code: 21244
Enter Zip+4 (optional)

E-mail Address: daisy.kittles@gmail.com
Confirm E-mail Address: daisy.kittles@gmail.com

Phone Number: 4102654137

User ID: dkittles123

Password:
Confirm Password:

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


What is a relative's telephone number that is not your own?
Security Question #2 Answer: own

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

Submit User [Cancel](#) **Step 9**

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.

Confirmation x

Your ID has been successfully registered with CMS Enterprise Portal. An e-mail has been sent to your registered e-mail address. You can now login by clicking [here](#)  **Step 10**

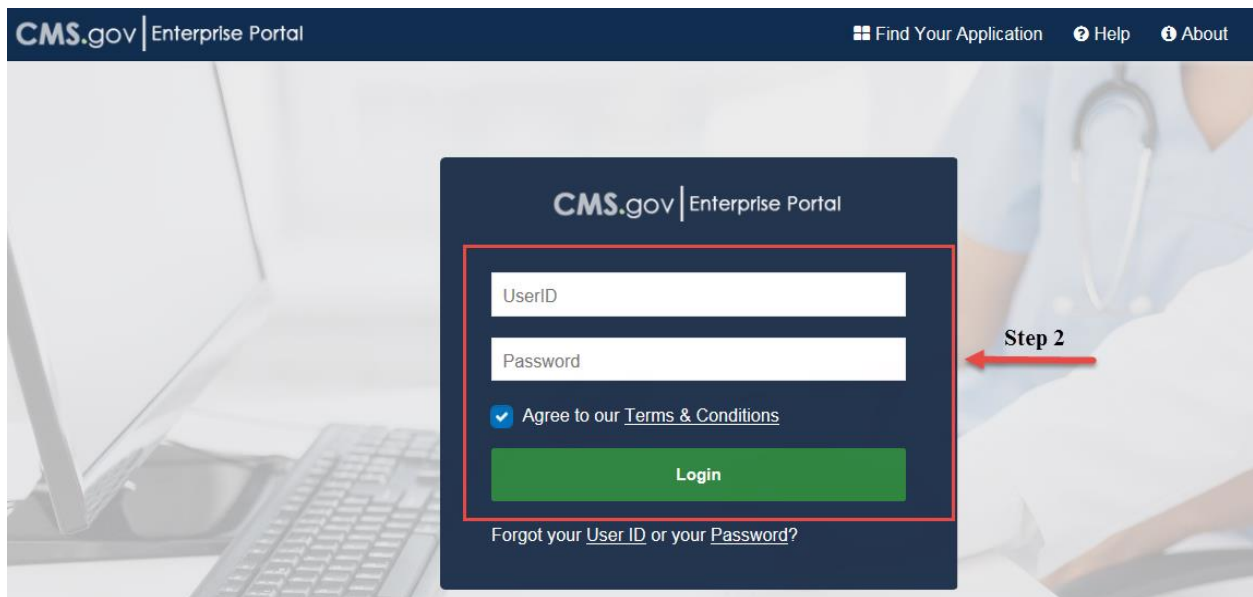
How to Set Up ACO Security Official (SO) Role

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.

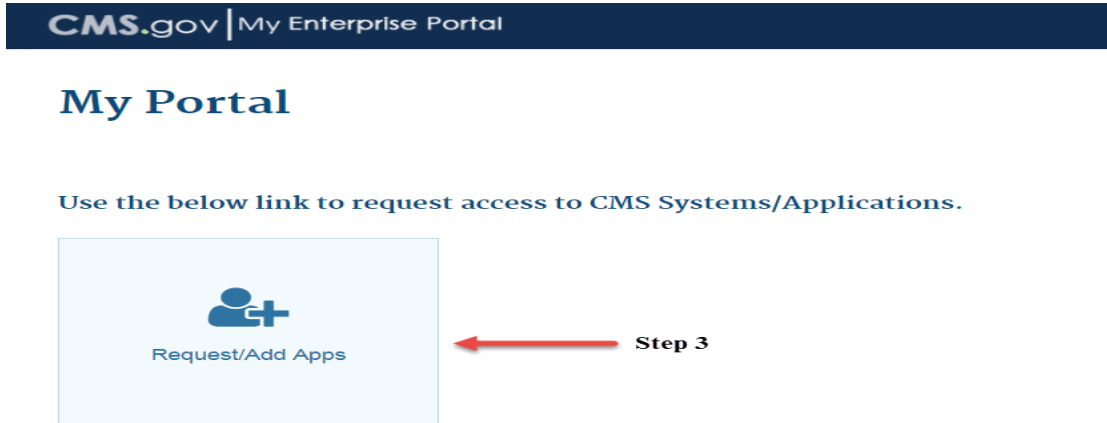
Important: You will not be able to log into the QPP Portal if your username includes an @ symbol. Please contact the Quality Payment Program by phone at 1-866-288-8292 / TTY 877-715-6222 or by email at gpp@cms.hhs.gov for assistance.

Steps to Create a New ACO SO Role:

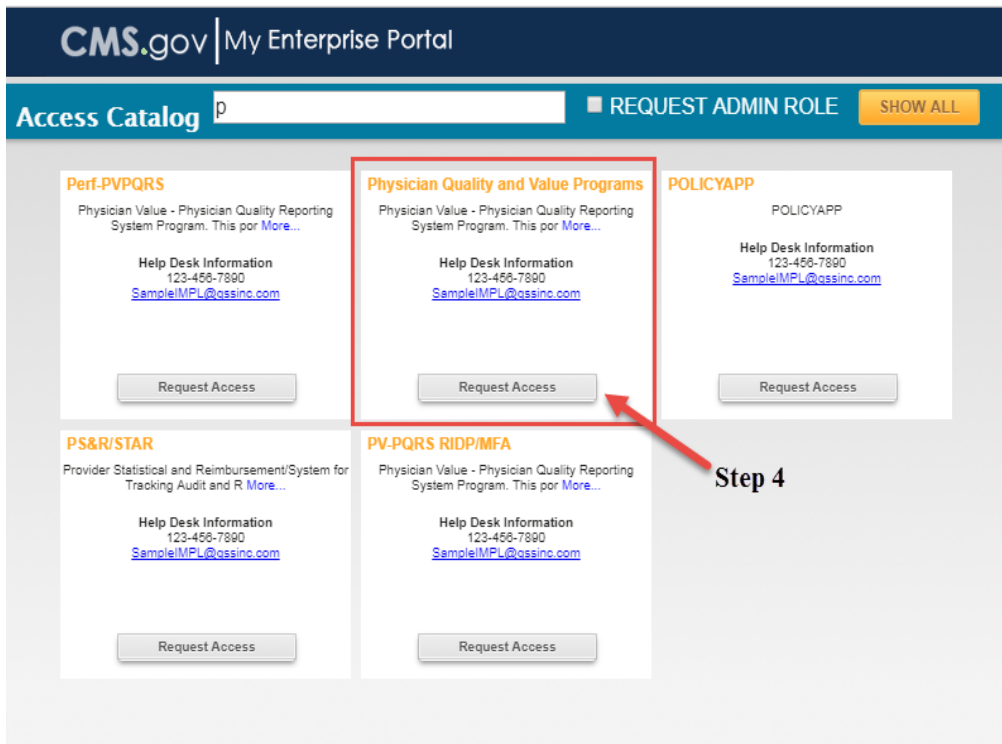
1. Navigate to <https://portal.cms.gov>. The CMS Enterprise Portal home page is displayed.
2. Once on the page, enter your user ID and password and agree to Terms and Conditions by clicking the checkbox.



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.'**



- 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.'**

The screenshot shows the 'Request New Application Access' form. On the left, there is a navigation menu with 'My Access' and 'Requests' sections. The main form area has a title 'Request New Application Access' and a '* Required Field' indicator. The 'Application Description' is set to 'Physician Quality and Value Programs'. Below this, there is a description: 'Physician Value - Physician Quality Reporting System Program. This portal allows access to applications such as Submissions, Web Interface, Feedback Dashboard and Reports and, if applicable, electing CAHPS.' The 'Select a Group' section has four radio button options: 'CMS/Help Desk User', 'PV Provider', 'Provider Approver', and 'PQRS Provider'. The 'Provider Approver' option is selected and highlighted with a red box. A red arrow points to this box with the text 'Step 5'. A 'Cancel' button is located at the bottom right of the form.

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

The screenshot shows the 'Request New Application Access' form at a later stage. The 'Application Description' remains 'Physician Quality and Value Programs'. The 'Select a Group' section now has four radio button options: 'PQRS Provider', 'PV Provider', 'Provider Approver', and 'CMS/Help Desk User'. The 'Provider Approver' option is selected. Below this, the 'Select a Role' section has a dropdown menu set to 'ACO Security Official'. The 'Role Description' is: 'Role for a Physician group to approve other users for that group for PQRS and PV-PQRS. To register in the PV-PQRS for PY 2014, view PY2013 registration data and view QRURs Reports (drill down, dashboard).' At the bottom, there is a note: 'This role requires Identity Verification and may require multi-factor authentication credentials to be set up. If your Level of Assurance has not been met for this role, you will be asked to provide additional information to verify your identity and if applicable, register a device for multi-factor authentication. Please select 'Next' to continue'. A red arrow points to the 'Next' button with the text 'Step 6'. A 'Cancel' button is also present.

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.

The screenshot shows a web interface for requesting application access. On the left is a sidebar with two main sections: 'My Access' and 'Requests'. Under 'My Access', there are links for 'View and Manage My Access' and 'Request New Application Access'. Under 'Requests', there is a link for 'My Pending Requests'. The main content area is titled 'Request New Application Access' and 'Identity Verification'. It contains a paragraph of introductory text, a numbered list of three instructions, and a final paragraph. At the bottom, the text 'Step 7' is followed by a red arrow pointing to a blue 'Next' button, with a blue 'Cancel' button to its right.

Request New Application Access

Identity Verification

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

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

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

Step 7 → **Next** **Cancel**

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.

Request New Application Access

Terms and Conditions

OMB No. 0938-1238 | Expiration Date: 04/30/2017 | [Paperwork Reduction Act](#)

Protecting Your Privacy

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

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

HHS Rules Of Behavior

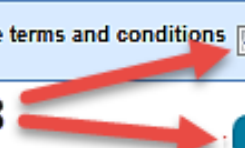
We encourage you to read the [HHS Rules of Behavior](#), which provides the appropriate use of all HHS information technology resources for Department users, including Federal employees, contractors, and other system users.

I have read the HHS Rules of Behavior (HHS RoB), version 2010-0002.001S, dated August 26 2010 and understand and agree to comply with its provisions. I understand that violations of the HHS RoB or information security policies and standards may lead to disciplinary action, up to and including termination of employment; removal or debarment from work on Federal contracts or projects; and/or revocation of access to Federal information, information systems, and/or facilities; and may also include criminal penalties and/or imprisonment. I understand that exceptions to the HHS RoB must be authorized in advance in writing by the OPDIV Chief Information Officer or his/her designee. I also understand that violation of laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS RoB draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

Identity Verification

I understand that the identity proofing services being requested are regulated by the Fair Credit Reporting Act and that my explicit consent is required to use these services. I understand that any special procedures established by CMS for identity proofing using Experian have been met and the services requested by CMS to Experian will be used solely to confirm the applicant's identity to avoid fraudulent transactions in the applicant's name.

I agree to the terms and conditions

Step 8 

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

Your Information

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

* First Name: Middle Name:

* Last Name: Suffix:

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

* E-mail Address:

Re-enter your E-mail address.

* Confirm E-mail Address:

Enter your full 9 digit social security number, as it may be required for Identity Verification.

Social Security Number:

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

* Date of Birth:

U.S. Home Address Foreign address
Enter your current or most recent home address, as it may be required for Identity Verification.

* Home Address Line 1:


Home Address Line 2:

* City: * State: * Zip Code: Zip Code Extension: Country: USA


Enter your primary phone number, as it may be required for Identity Verification.

* Primary Phone Number:

Step 9



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.


Your Information **Verify Your Identity**

Verify Identity

You may have opened a mortgage loan in or around August 2012. Please select the lender to whom you currently make your mortgage payments. If you do not have a mortgage, select 'NONE OF THE ABOVE/DOES NOT APPLY'.

- SUN WEST MTG
- NORVEST BANK
- INDEPENDENT MTG
- PARKWAY MTG
- NONE OF THE ABOVE/DOES NOT APPLY

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

- DRP COINS
- ENGR CUSTOM PLASTIC
- SOUTH JERSEY GAS CO
- US MARINES
- NONE OF THE ABOVE/DOES NOT APPLY

According to our records, you previously lived on (7TH). Please choose the city from the following list where this street is located.

- VIRGINIA
- CHISHOLM
- WINONA
- GRAND RAPIDS
- NONE OF THE ABOVE/DOES NOT APPLY

Please select the number of bedrooms in your home from the following choices. If the number of bedrooms in your home is not one of the choices please select 'NONE OF THE ABOVE'.

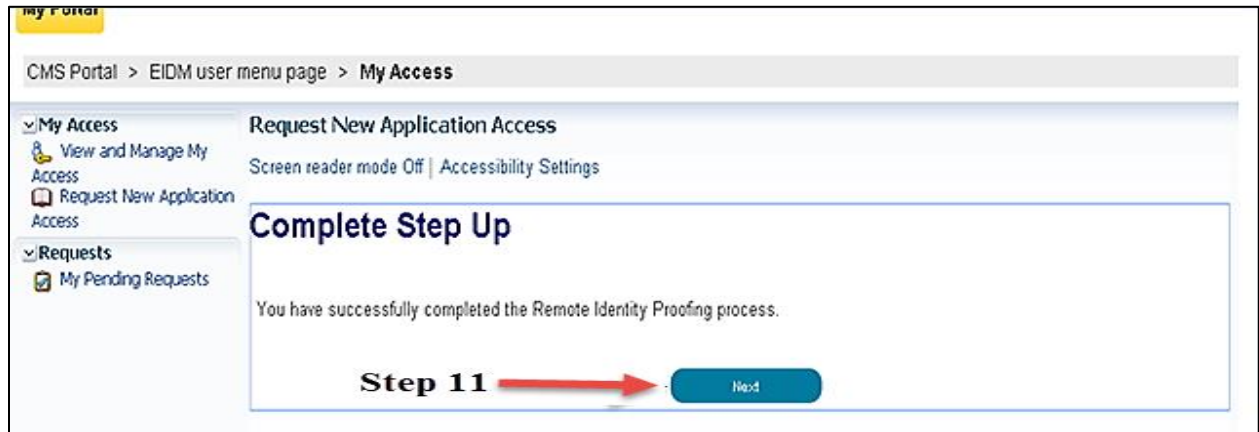
- 2
- 3
- 4
- 5
- NONE OF THE ABOVE/DOES NOT APPLY

Please select the county for the address you provided.

- BERGEN
- CAMDEN
- ATLANTIC
- MORRIS
- NONE OF THE ABOVE/DOES NOT APPLY

Step 10

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.

CMS.gov My Enterprise Portal Welcome ▾ Da

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: 4885564444, 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 for logging into your application.

• MFA Device Type: menu below.

- Select MFA Device Type
- Phone/Tablet/PC/Laptop
- E-mail
- Text Message-Short Message Service(SMS)
- Interactive Voice Response(IVR)

Next **Cancel**

Step 13

- 
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) 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

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:

Enter the alphanumeric code that displays under the label Credential ID on your device.

* Credential ID:

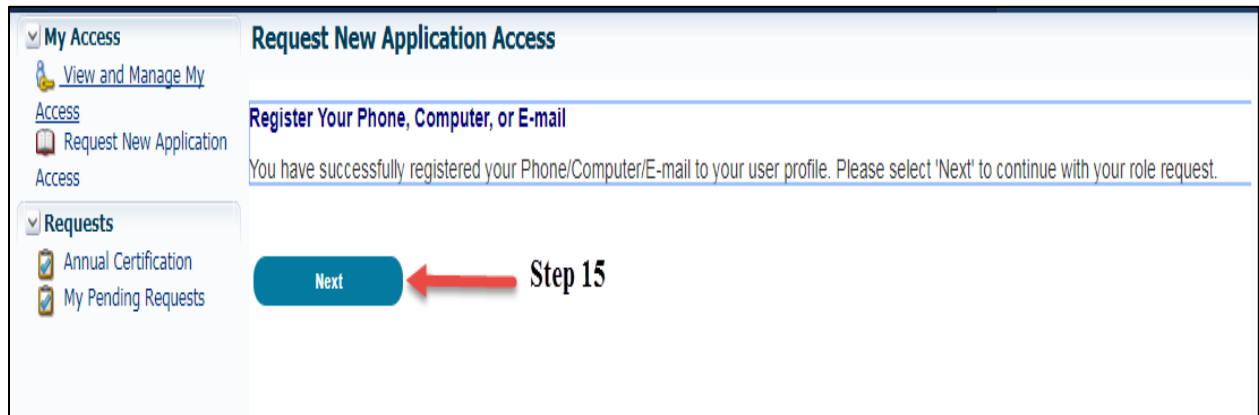
* MFA Device Description:

Next

Cancel

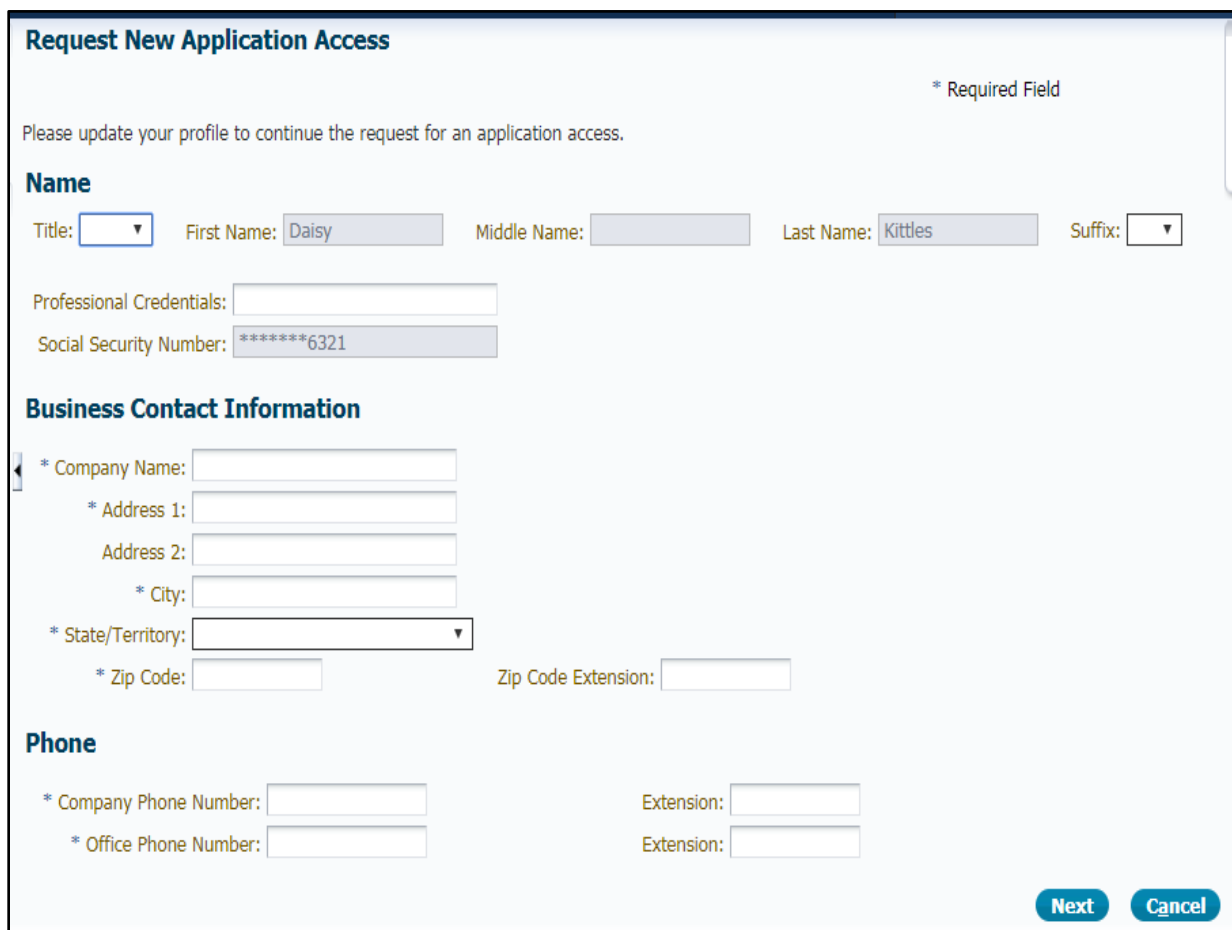
Step 14

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



The screenshot shows a web interface titled "Request New Application Access". On the left, there is a navigation menu with sections "My Access" and "Requests". Under "My Access", there are links for "View and Manage My Access" and "Request New Application Access". Under "Requests", there are links for "Annual Certification" and "My Pending Requests". The main content area has a sub-header "Register Your Phone, Computer, or E-mail" and a message: "You have successfully registered your Phone/Computer/E-mail to your user profile. Please select 'Next' to continue with your role request." A blue button labeled "Next" is visible, with a red arrow pointing to it from the text "Step 15" to its right.

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.



The screenshot shows the "Request New Application Access" page with a form for updating profile information. The page title is "Request New Application Access" and there is a note: "* Required Field". The main instruction is "Please update your profile to continue the request for an application access." The form is divided into several sections:

- Name:** Includes fields for Title (dropdown), First Name (Daisy), Middle Name, Last Name (Kittles), and Suffix (dropdown). There are also fields for Professional Credentials and Social Security Number (*****6321).
- Business Contact Information:** Includes fields for Company Name, Address 1, Address 2, City, State/Territory (dropdown), Zip Code, and Zip Code Extension.
- Phone:** Includes fields for Company Phone Number and Office Phone Number, each with an Extension field.

At the bottom right, there are "Next" and "Cancel" buttons.

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 ACO's Primary 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).

The screenshot shows the CMS.gov My Enterprise Portal interface for creating a new ACO organization. The page title is "Create New ACO Organization". The user is logged in as "Tom Cat". The form is titled "Create/Associate" and has two options: "Associate to an Existing Organization" and "Create an Organization". The "Create an Organization" option is selected, indicated by a red arrow. A red box highlights the form fields, which include:

- * Primary TIN: Shared Savings Program and Pioneer: ACO's Primary Tax Identification Number (TIN)
- * ACO ID: ACO ID issued by CMS
- * Legal Business Name: [Text Field]
- * Program Type: Shared Savings Program (08) [Dropdown]
- * ACO Participant ID 1: Shared Savings Program and Pioneer: ACO's Participant Tax Identification Number (TIN)
- * ACO Participant ID 2: Shared Savings Program and Pioneer: ACO's Participant Tax Identification Number (TIN)
- ACO Participant ID 3: Shared Savings Program and Pioneer: ACO's Participant Tax Identification Number (TIN)
- * Address Line 1: [Text Field] Address Line 2: [Text Field]
- * City: [Text Field] * State: [Dropdown]
- * Zip Code: [Text Field] Zip Code Extension: [Text Field]
- Country: United States
- * Phone Number: [Text Field] Extension: [Text Field]
- Fax Number: [Text Field]
- Email: [Text Field]
- Website: [Text Field]
- * Reason for Request: [Text Area]

At the bottom right of the form, there are "Next" and "Cancel" buttons. A red arrow points to the "Next" button.

Request New Application Access Associate to Existing ACO Organization * Required Field

Application Description:

Physician Value - Physician Quality Reporting System Program. This portal allows access to applications such as Submissions, Web Interface, Feedback Dashboard and Reports and, if applicable, electing CAHPS.

Select a Group: CMS/Help Desk User
 PV Provider
 Provider Approver
 PQRS Provider

Select a Role:

Role Description: Role for a Physician group to approve other users for that group for PQRS and PV-PQRS. To register in the PV-PQRS for PY 2014, view PY2013 registration data and view QRURs Reports (drill down, dashboard).

* Create/Associate: Associate to an Existing Organization Create an Organization

Please provide the complete Medicare billing Tax Identification Number (TIN); or the Legal Business Name (LBN) and State; or the LBN and Street Address to perform the organization search.

Legal Business Name:

TIN:

Address Line 1: Address Line 2:

City: State:

Zip Code: Zip Code Extension:

* Organization:

* Reason for Request:

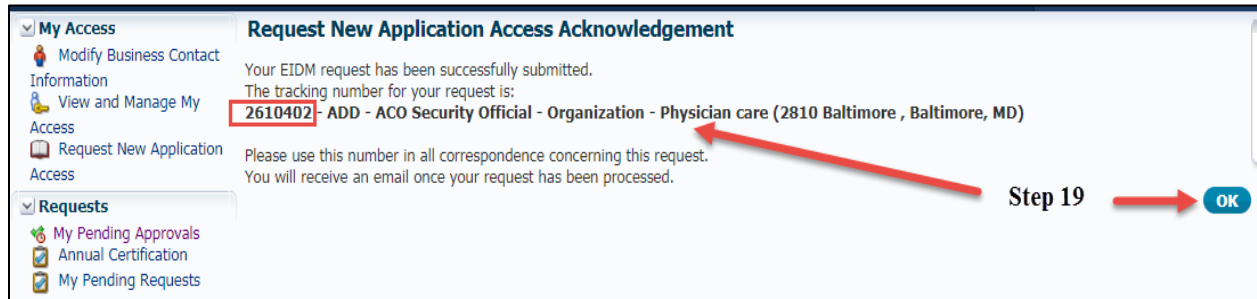
NOTE: Please use the ACO's Legal Business Name and the ACO's Primary TIN when completing the Legal Business Name and TIN fields, respectively.

NOTE: Make sure that the search criteria entered is accurate. If the organization is unable to be found, contact the QPP Service Center 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 QPP Service Center, 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.

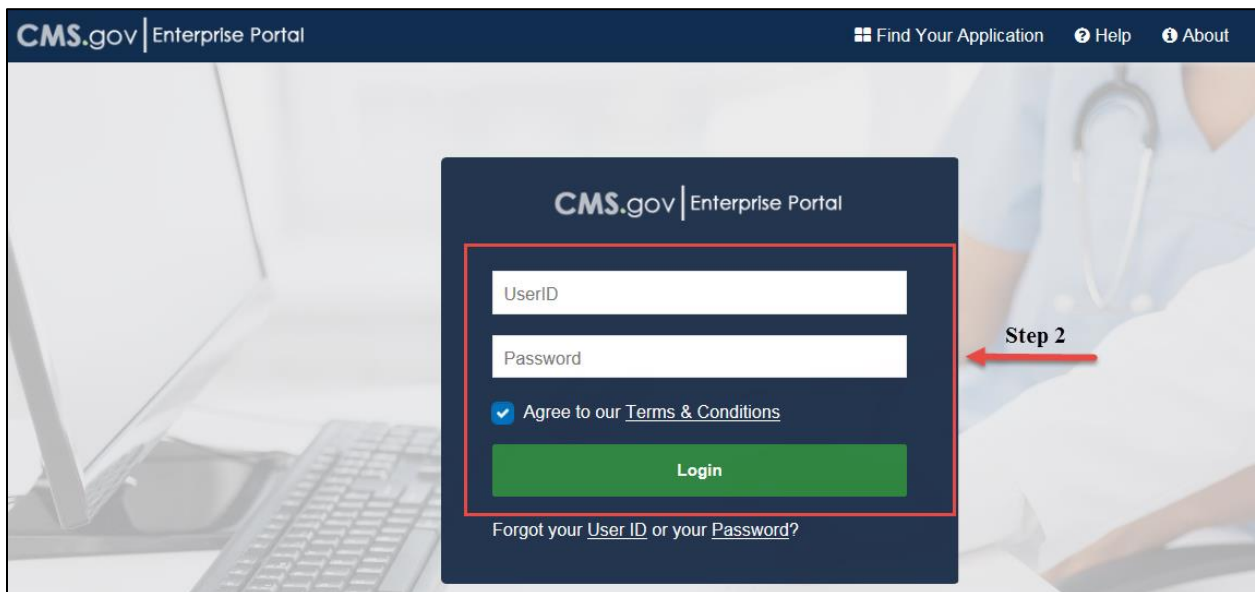
The notification of approval, denial, or other requests will be sent to the role requestor's email address on file for the request.

How to Set Up the Web Interface Submitter Role

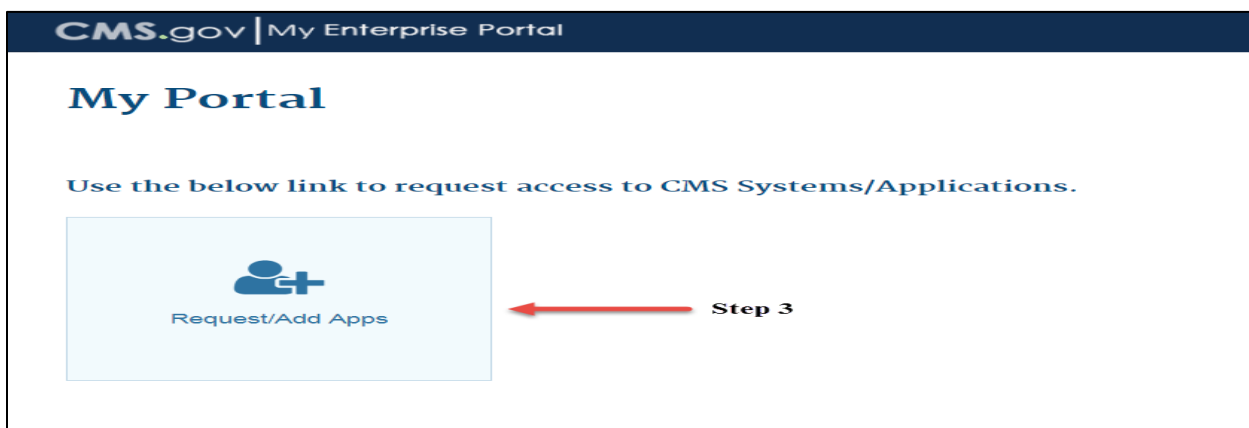
After an ACO SO role has been created and approved, a Web Interface Submitter Role must be established. The Web Interface Role cannot be set up until there is at least one ACO SO role set up.

Steps to Create a Web Interface Submitter Role:

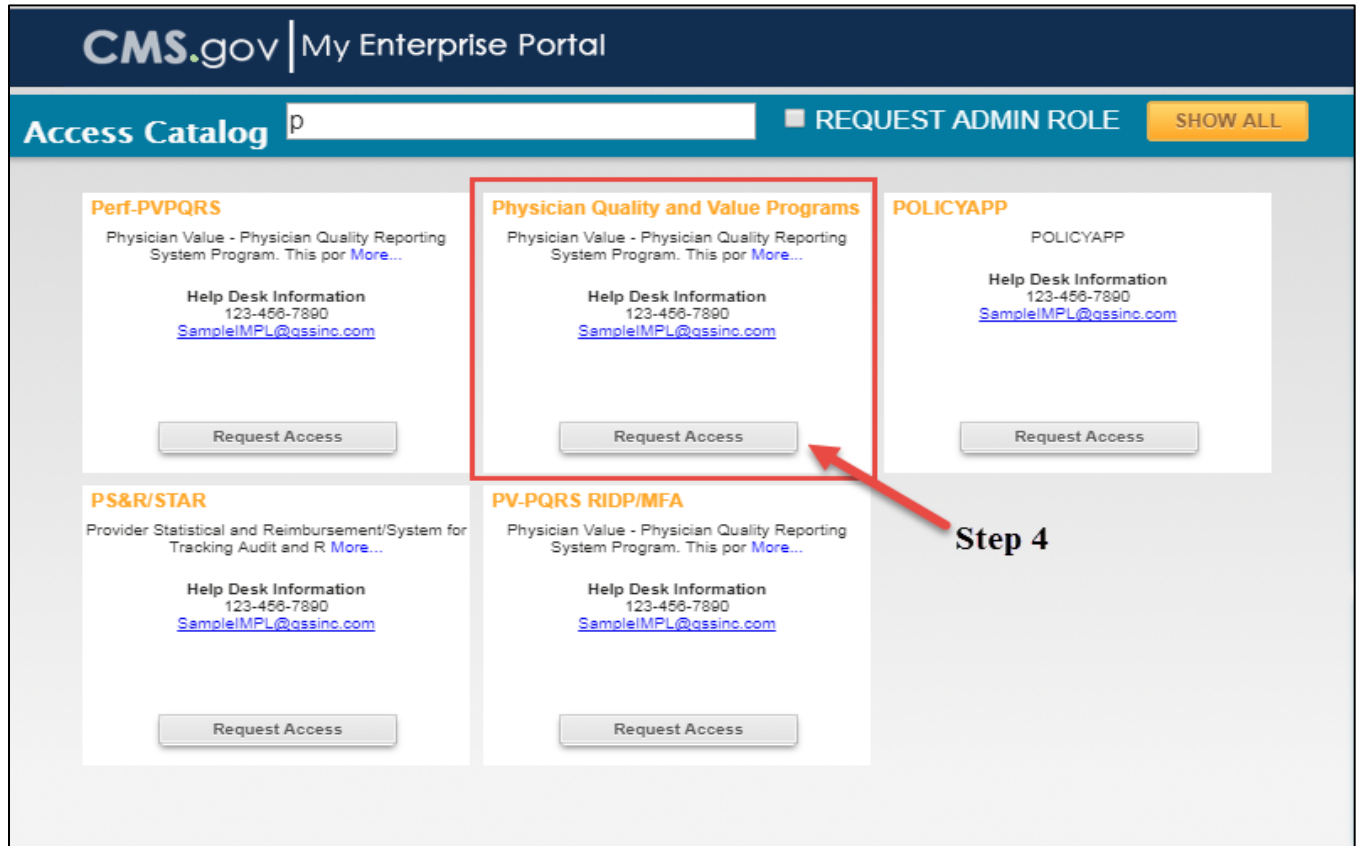
1. Navigate to <https://portal.cms.gov>. The CMS Enterprise Portal page is displayed.
2. Once on the page, enter your user ID and password and agree to Terms and Conditions by clicking the checkbox.



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.

The screenshot shows the 'Request New Application Access' form. The 'Application Description' is set to 'Physician Quality and Value Programs'. Under 'Select a Group', 'PQRS Provider' is selected. The 'Select a Role' dropdown menu is open, showing the following options: User Roles, PQRS Submitter, PQRS Representative, **Web Interface Submitter** (highlighted), Individual Practitioner Representative, and Physician Quality Initiatives Portal (PQIP) Group Representative. A 'Cancel' button is visible on the right.

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.

The screenshot shows the 'Request New Application Access' form at the 'Identity Verification' step. The text reads: 'To protect your privacy, you will need to complete Identity Verification successfully, before requesting access to the selected role. Below are a few items to keep in mind.' The instructions are:

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

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

Step 7 → **Next** Cancel

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

Request New Application Access

Terms and Conditions

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

Protecting Your Privacy

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

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

HHS Rules Of Behavior


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

I have read the HHS Rules of Behavior (HHS RoB), version 2010-0002.001S, dated August 26 2010 and understand and agree to comply with its provisions. I understand that violations of the HHS RoB or information security policies and standards may lead to disciplinary action, up to and including termination of employment; removal or debarment from work on Federal contracts or projects; and/or revocation of access to Federal information, information systems, and/or facilities; and may also include criminal penalties and/or imprisonment. I understand that exceptions to the HHS RoB must be authorized in advance in writing by the OPD/IV Chief Information Officer or his/her designee. I also understand that violation of laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS RoB draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

Identity Verification

I understand that the identity proofing services being requested are regulated by the Fair Credit Reporting Act and that my explicit consent is required to use these services. I understand that any special procedures established by CMS for identity proofing using Experian have been met and the services requested by CMS to Experian will be used solely to confirm the applicant's identity to avoid fraudulent transactions in the applicant's name.

I agree to the terms and conditions :

Step 8 

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

Your Information

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

• First Name: Middle Name:

• Last Name: Suffix:

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

• E-mail Address:

Re-enter your E-mail address.

• Confirm E-mail Address:

Enter your full 9 digit social security number, as it may be required for Identity Verification.

Social Security Number:

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

• Date of Birth:

U.S. Home Address Foreign address
Enter your current or most recent home address, as it may be required for Identity Verification.

• Home Address Line 1:


Home Address Line 2:

• City: • State: • Zip Code: Zip Code Extension: Country: USA

Enter your primary phone number, as it may be required for Identity Verification.

• Primary Phone Number:

Step 9



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.

Your Information **Verify Your Identity**

Verify Identity

You may have opened a mortgage loan in or around August 2012. Please select the lender to whom you currently make your mortgage payments. If you do not have a mortgage, select 'NONE OF THE ABOVE/DOES NOT APPLY'.

- SUN WEST MTG
- NORVEST BANK
- INDEPENDENT MTG
- PARKWAY MTG
- NONE OF THE ABOVE/DOES NOT APPLY

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

- DRP CONS
- ENGR CUSTOM PLASTIC
- SOUTH JERSEY GAS CO
- US MARINES
- NONE OF THE ABOVE/DOES NOT APPLY

According to our records, you previously lived on (7TH). Please choose the city from the following list where this street is located.

- VIRGINIA
- CHISHOLM
- WINONA
- GRAND RAPIDS
- NONE OF THE ABOVE/DOES NOT APPLY

Please select the number of bedrooms in your home from the following choices. If the number of bedrooms in your home is not one of the choices please select 'NONE OF THE ABOVE'.

- 2
- 3
- 4
- 5
- NONE OF THE ABOVE/DOES NOT APPLY

Please select the county for the address you provided.

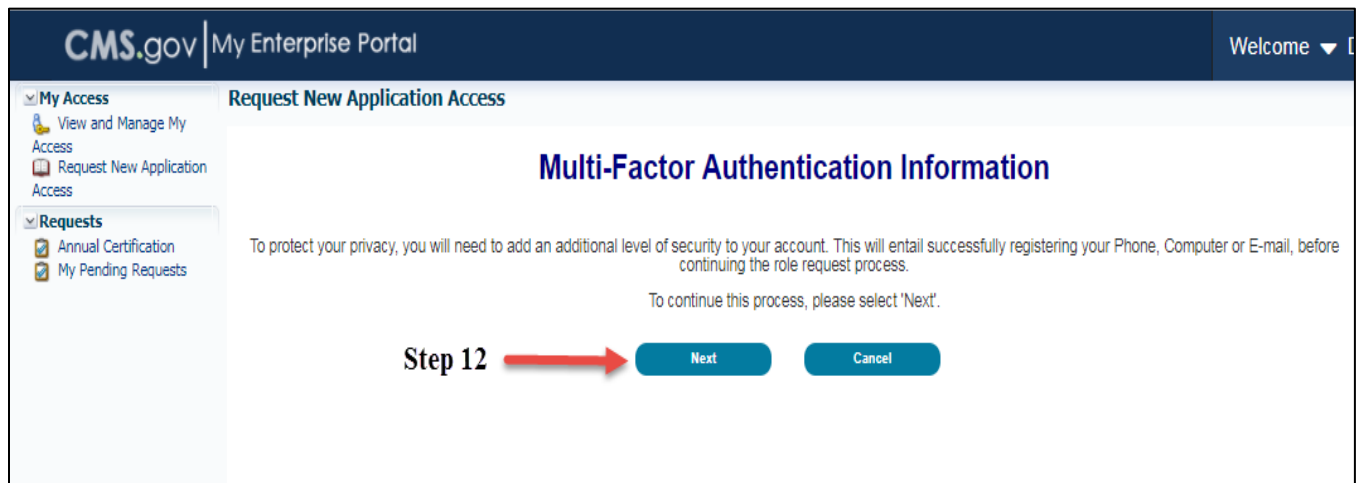
- BERGEN
- CAMDEN
- ATLANTIC
- MORRIS
- NONE OF THE ABOVE/DOES NOT APPLY

Step 10

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.

The screenshot shows the CMS.gov My Enterprise Portal interface. The main heading is "Register Your Phone, Computer, or E-mail". Below this, there are instructions for adding a Security Code (MFA) to the login. The instructions are organized into sections:

- 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.vio.svmantec.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:
 - , (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.

At the bottom of the page, there is a form with a dropdown menu labeled "MFA Device Type:". The dropdown menu is open, showing the following options: "Select MFA Device Type", "Phone/Tablet/PC/Laptop", "E-mail", "Text Message-Short Message Service(SMS)", and "Interactive Voice Response(IVR)". A red arrow points to the dropdown menu, labeled "Step 13".

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**'.

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:

* Credential ID :

* MFA Device Description:

Step 14

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

Request New Application Access

Register Your Phone, Computer, or E-mail

You have successfully registered your Phone/Computer/E-mail to your user profile. Please select 'Next' to continue with your role request.

Step 15

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

Request New Application Access * Required Field

Please update your profile to continue the request for an application access.

Name

Title: First Name: Middle Name: Last Name: Suffix:

Professional Credentials:

Social Security Number:

Business Contact Information

* Company Name:

* Address 1:

Address 2:

* City:

* State/Territory:

* Zip Code: Zip Code Extension:

Phone

* Company Phone Number: Extension:

* Office Phone Number: Extension:

Step 16 ←

→ **Next** **Cancel**

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's Legal Business Name and the ACO's Primary TIN when completing the Legal Business Name and TIN fields respectively.

Request New Application Access * Required Field

Application Description:

Physician Value - Physician Quality Reporting System Program. This portal allows access to applications such as Submissions, Web Interface, Feedback Dashboard and Reports and, if applicable, electing CAHPS.

Select a Group: PQRS Provider
 PV Provider
 Provider Approver
 CMS/Help Desk User

Select a Role:

Role Description: Allows access to the GPRO and ACO Web Interface for data abstraction and submission.

Please provide the complete Medicare billing Tax Identification Number (TIN); or the Legal Business Name (LBN) and State; or the LBN and Street Address to perform the organization search.

Legal Business Name:

TIN:

Address Line 1: Address Line 2:

City: State:

Zip Code: Zip Code Extension:

* Reason for Request:

Step 17

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.

Request New Application Access Review * Required Field

Application Description:
Physician Value - Physician Quality Reporting System Program. This portal allows access to applications such as Submissions, Web Interface, Feedback Dashboard and Reports and, if applicable, electing CAHPS.

Group Selected: PQRS Provider
Role Selected: Web Interface Submitter
Role Description: Allows access to the GPRO and ACO Web Interface for data abstraction and submission.

Name
Title:
First Name: Middle Name: Last Name: Suffix:
Professional Credentials:
Social Security Number:

Business Contact Information
Company Name:
Address 1:
Address 2:
City:
State/Territory:
Zip Code: Zip Code Extension:

Phone
Company Phone Number: Extension:
Office Phone Number: Extension:

Please provide the complete Medicare billing Tax Identification Number (TIN); or the Legal Business Name (LBN) and State; or the LBN and Street Address to perform the organization search.
Organization:
Reason for Request:

Step 18 →

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.

Request New Application Access Acknowledgement

Your EIDM request has been successfully submitted.
The tracking number for your request is:
2610419 - ADD - Web Interface Submitter - Organization - Test Automation (2810 lord baltimore, Baltimore, MD)

Please use this number in all correspondence concerning this request.
You will receive an email once your request has been processed.

Step 19 →



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.

CMS.gov | Enterprise Portal Find Your Application

CMS.gov | Enterprise Portal

UserID

Password

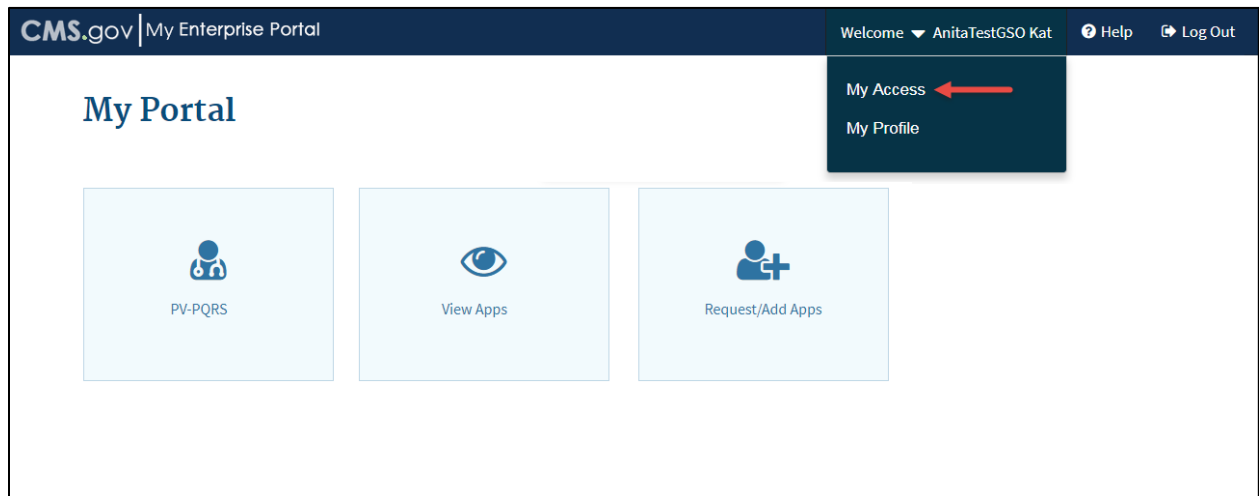
Choose MFA Device

[Trouble Accessing Security Code?](#)

Agree to our [Terms & Conditions](#)

Forgot your [User ID](#) or your [Password](#)?

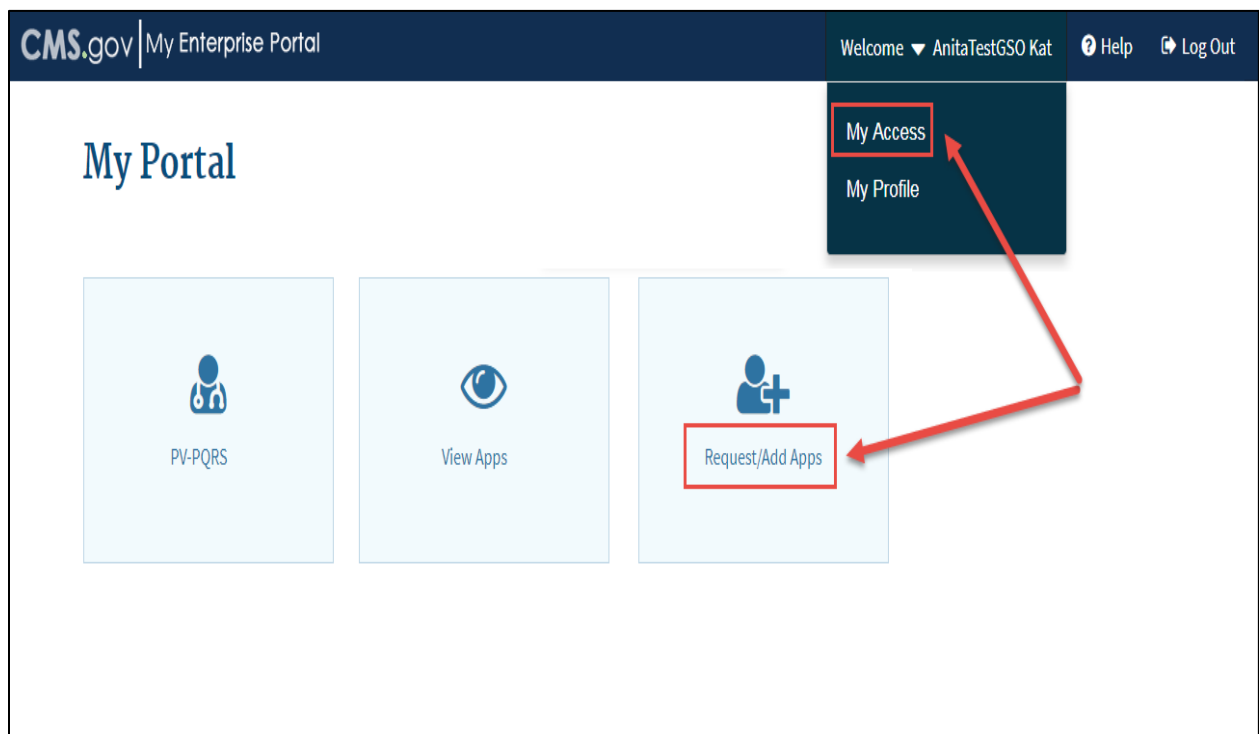
2. After successfully logging into the CMS Enterprise Portal using your EIDM user ID, password, and completing MFA process, **click on Welcome <Your Name>** at the top right of your screen. Once selected, a dropdown will allow you to then **click on My Access**.



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



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



- The screen will display your 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.

The screenshot shows the CMS.gov My Enterprise Portal interface. The top navigation bar includes the CMS.gov logo, 'My Enterprise Portal', 'My Apps', and a user welcome message 'Welcome AnitaTestGSO'. The left sidebar contains navigation menus for 'My Access', 'Requests', and 'Administration'. The main content area is titled 'Request to Remove Physician Quality and Value Programs Role' and includes instructions on how to remove a role. Below the instructions is a table titled 'My Role Information:' with three columns: 'My Roles', 'Existing Role Details', and 'Remove a Role'. The table lists two roles: 'Web Interface Submitter' and 'PQRS Submitter'. A 'Cancel' button is located below the table. A 'Confirmation' pop-up dialog is displayed in the foreground, asking 'Are you sure you want to remove this role?' and providing instructions on how to proceed. The dialog has 'OK' and 'Cancel' buttons.

Request to Remove Physician Quality and Value Programs Role

To remove a role from an application, click the Remove a Role link. You can only remove one role at a time. Once a role is removed from an application, you will need to request access again to have it restored.

My Role Information:

My Roles	Existing Role Details	Remove a Role
Web Interface Submitter	TestNGC (2810 lord baltimore dr, Windosr, MD)	Remove
PQRS Submitter	My Home (Test, Columbia, MD)	Remove

Cancel

Confirmation

Are you sure you want to remove this role?

Once the role is removed, you will need to request access again to have it restored. Select 'OK' to continue, Otherwise, select 'Cancel'.

OK Cancel



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.