Quality Payment PROGRAM

Guide for Obtaining an EIDM Account and 'Physician Quality and Value Programs' Role for the Quality Payment Program (QPP)

Table of Contents

I. Introduction 2
II. Who Needs an EIDM account and 'Physician Quality and Value Programs' Role for QPP? 3
III. Which Role Do I Need? 6
IV. What Do I Do Now? 13
V. Creating an EIDM Account 15
VI. Requesting an Approver Role 20
VII. Requesting a Provider Role 40

I. Introduction

This guide is for users who need an Enterprise Identity Data Management (EIDM) account and/or 'Physician Quality and Value Program' role to submit or access QPP data. This guide provides:

1. Guidance about the users who need an EIDM account and 'Physician Quality and Value Program' role
2. Guidance for choosing the right role for your needs
3. Step-by-step instructions for users to create an EIDM account in the CMS Enterprise Portal
4. Step-by-step instructions for users to request a role in the CMS Enterprise Portal using their existing EIDM account

Note: This guide was updated on July 2018 to include information for accessing MIPS performance feedback and submitting targeted reviews for the 2017 performance year.

What's Changing?

Clinicians and third-party organizations who have reported to the Physician Quality Reporting System (PQRS) will recognize the EIDM roles needed for submission. (Please note that EIDM has retained the PQRS naming convention for roles associated with QPP submission.) However, there are a few changes to the users who will need EIDM accounts and how they will request the necessary roles:

1. While Accountable Care Organizations (ACOs) will continue to obtain an EIDM account and role to report Quality data at the entity level, **groups participating in a Shared Savings Program (SSP) ACO** must obtain their own EIDM accounts and roles under their Participant TIN to submit and meet the Advancing Care Information requirements under MIPS for purposes of the MIPS APM Scoring Standard and the Shared Savings Program ACO-11 quality measure.
2. **Electronic Health Record (EHR) or other Health IT Vendors** reporting data on behalf of their clients will need to secure the appropriate EIDM role for **each TIN** (group or individual clinicians) they're reporting on behalf of; this does not apply to Health IT vendors who are CMS-approved Qualified Clinical Data Registries or Qualified Registries.
3. **Groups (including MIPS APMs), Comprehensive Primary Care Plus (CPC+) practices, and individual practitioners that have contracted with an EHR/Health IT Vendor to report data on their behalf** will need to appoint an authorized representative to obtain an EIDM account with a Provider Approver role to approve the submitter role for the Vendor.
4. **NEW: Beginning with the 2018 Performance Year, a Security Official role is required to register a group for the CMS Web Interface and/or CAHPS for MIPS survey**.

II. Who Needs an EIDM account and 'Physician Quality and Value Programs' Role for QPP?

1. Clinicians, groups, MIPS APMs, and certain Advanced APM participants that:
    - Will be submitting data directly to qpp.cms.gov
    - Have secured an EHR/Health IT Vendor to submit their data to qpp.cms.gov (other than a CMS-approved Qualified Clinical Data Registry or Qualified Registry)
    - Want to view the data submitted on their behalf by a third party
    - Want to register their group for the CMS Web Interface and/or the CAHPS for MIPS survey (groups only)
    - Want to review MIPS performance feedback and/or submit a targeted review request
        - ♦ With the exception of SSP ACOs, SSP participant TINs, and Next Generation ACOs, MIPS APM Entities with clinicians scored under the APM scoring standard will not be able to access their MIPS feedback by logging into qpp.cms.gov, and therefore will not need to get EIDM accounts to access performance feedback or submit a targeted review request.
        - ♦ Only users with an EIDM role for a practice (TIN) or ACO entity will be able to log in and view performance feedback for that practice or entity. Third party intermediaries with an EIDM account and role only associated with their own business organization will not be able to use those credentials to log in and view performance feedback for their clients.
2. Qualified Clinical Data Registries, Qualified Registries, and EHR/Health IT Vendors that will be submitting data directly to qpp.cms.gov on behalf of their clients.

All EIDM account holders must be in the United States of America

Who?	Why?
Accountable Care Organizations (ACOs): Shared Savings Program (SSP) (Primary TIN)	ACO representatives that will be accessing qpp.cms.gov to report Quality data through the CMS Web Interface on behalf of the entire ACO, access the ACO's MIPS performance feedback and payment adjustment information, or submit a targeted review request. **Note:** Guidance for requesting ACO entity level EIDM roles is available in the 2017 EIDM ACO User Guide. **IMPORTANT!** Groups participating in a Shared Savings Program (SSP) ACO must obtain EIDM accounts and roles

Who?	Why?
	under their Participant TIN to submit and meet the Advancing Care Information requirements under MIPS for purposes of the MIPS APM Scoring Standard and the Shared Savings Program ACO-11 quality measure. (Note that the Participant TIN must be different than the ACO Primary TIN for EIDM registration. Single TIN ACOs can review role request verification guidance on page 24 of the 2017 EIDM ACO User Guide.)
ACOs: Next Generation (NGACO) (Primary TIN)	ACO representatives that will be reporting Quality data through the CMS Web Interface on behalf of the entire ACO **Note:** For 2017 QPP guidance on EIDM registration and roles, please review NGACO EIDM guidance at https://app.innovation.cms.gov/NGACOConnect/ Questions on EIDM can be sent to NextGenerationACOModel@cms.hhs.gov
Comprehensive Primary Care Plus (CPC+) (The designated CPC+ practice defined by a practice site location, TINs/NPIs)	1. CPC+ practices that will be **submitting CPC+ Quality data directly** via file upload on qpp.cms.gov: **Note:** Please send questions about the EIDM roles needed for eCQM attestation through the CPC+ Practice Portal to CPCplus@telligen.com 2. CPC+ practices that have **secured an EHR/Health IT Vendor to submit data on their behalf** (those that are not a CMS-approved Qualified Clinical Data Registry or Qualified Registry) CPC+ representatives that want to **view data submitted on their behalf** by an EHR/Health IT Vendor
Groups, including: • **MIPS APM participants** • **Non-QP Advanced APM participants** *(2+ clinicians billing under the TIN)*	1. Group or clinician representatives that will be submitting MIPS data directly to qpp.cms.gov including data for any, or all, of the following Performance Categories (individual or group reporting): ○ **Quality** (via file upload or CMS Web Interface) ○ **Advancing Care Information** (via file upload, attestation, or CMS Web Interface)

Who?	Why?
	○ **Improvement Activities** (via file upload, attestation, or CMS Web Interface) **IMPORTANT!** Groups participating in a Shared Savings Program (SSP) ACO must obtain EIDM accounts and roles to submit and meet the Advancing Care Information requirements under MIPS for purposes of the MIPS APM Scoring Standard and the Shared Savings Program ACO-11 quality measure. 2. Groups, reporting as individuals or a group, that **have secured an EHR/Health IT Vendor to submit data on their behalf** (those that are not a CMS-approved Qualified Clinical Data Registry or Qualified Registry) 3. Group representatives that want to **view data submitted on their behalf** (reporting as individuals or a group) by a Qualified Clinical Data Registry (QCDR), Qualified Registry, or EHR/Health IT Vendor 4. Group or clinician representatives that want to view MIPS performance feedback and payment adjustment information, and submit a targeted review request 5. Group representatives that want to register their group (or cancel a registration) for the CMS Web Interface and/or CAHPS for MIPS survey (refer to the 2018 Registration Guide for the CMS Web Interface and CAHPS for MIPS Survey for more information)
Individual/Solo Practitioners, including • **MIPS APM participants** • **Non-QP Advanced APM participants** *(1 clinician billing under the TIN/SSN)*	1. Individual practitioners (or their representatives) that will be **submitting MIPS data directly** to qpp.cms.gov including data for any, or all, of the following Performance Categories: ○ **Quality** (via file upload) ○ **Advancing Care Information** (via file upload or attestation) ○ **Improvement Activities** (via file upload or attestation) 2. Individual practitioners (or their representatives) that have **secured an EHR/Health IT Vendor to submit data on their behalf** (those that are not a CMS-approved Qualified Clinical Data Registry or Qualified Registry)

Who?	Why?
	3. Individual practitioners (or their representatives) that want to **view data submitted on their behalf** by a Qualified Clinical Data Registry (QCDR), Qualified Registry, or EHR/Health IT Vendor 4. Individual practitioners (or their representatives) that want to view MIPS performance feedback and payment adjustment information, and submit a targeted review request
Qualified Clinical Data Registries (QCDRs) **Qualified Registries** **EHR/Health IT Vendors**	Third party organizations ***submitting MIPS data directly*** to qpp.cms.gov on behalf of their clients (CPC+ practices, group practices and/or individual practitioners) including data for any, or all, of the following Performance Categories: • **Quality** (via QPP JSON/XML or QRDA III XML file upload) • **Advancing Care Information** (via QPP JSON/XML or QRDA III XML file upload) • *Improvement Activities* (via QPP JSON/XML or QRDA III XML file upload) **NOTE:** An EIDM role is not necessary for data submission via Application Program Interface (API) by QCDRs and Qualified Registries. Please visit the Developer Tools section of qpp.cms.gov for additional information on API submission.

III. Which Role Do I Need?

For 2017 Quality Payment Program data submission, users will continue to request the same roles that were needed to submit data to the Physician Quality Reporting System (PQRS).

Please note: Even though the EIDM naming convention still refers to "PQRS", these are the roles needed for QPP submission.

Who?	EIDM Role	EIDM Role Type	Functions
	ACO Security Official	Provider Approver	Please see the 2017 ACO EIDM Registration Guide for

Who?	EIDM Role	EIDM Role Type	Functions
ACOs: Shared Savings Program (SSP) (Primary TIN)	**Web Interface Submitter**	PQRS Provider	guidance on these roles. The Registration Guide is on the ACO Portal, accessible through the CMS Enterprise Portal. It is listed under "2017 Quality Measurement and Reporting Guides."
	IMPORTANT! Groups participating in a Shared Savings Program (SSP) ACO must obtain EIDM accounts and roles under their Participant TIN to submit and meet the Advancing Care Information requirements under MIPS for purposes of the MIPS APM Scoring Standard and the Shared Savings Program ACO-11 quality measure. **Please refer to the "Groups" section of this table for the roles needed.**		
ACOs: Next Generation (NGACO) (Primary TIN)	For 2017 QPP guidance on EIDM registration and roles, please review NGACO EIDM guidance at https://app.innovation.cms.gov/NGACOConnect/ Questions on EIDM can be sent to NextGenerationACOModel@cms.hhs.gov		
Comprehensive Primary Care Plus (CPC+) Practices The designated CPC+ TIN (2+ clinicians billing under the TIN)	**Security Official**	Provider Approver	• Approve "PQRS Submitter" role requests by other EIDM account holders for their organization (including EHR/Health IT Vendors reporting on behalf of their practice) • Submit data on behalf of the CPC+ practice • View all data submitted by/on behalf of the CPC+ practice

Who?	EIDM Role	EIDM Role Type	Functions
	PQRS Submitter	PQRS Provider	• Submit any MIPS data on behalf of the CPC+ practice • View all data submitted by/on behalf of the practice **Note:** An organization must have a Security Official before a user can request the PQRS Submitter role
Comprehensive Primary Care Plus (CPC+) Practices – Individual/Solo Practitioners *(1 clinician billing under the TIN/SSN)*	**Individual Practitioner**	Provider Approver	• Approve "PQRS Submitter" role requests by EIDM account holders for the clinician (including EHR/Health IT Vendors reporting on behalf of the clinician) • Submit data on behalf of the clinician • View all data submitted by/on behalf of the clinician
	Individual Practitioner Representative	PQRS Provider	• Submit any MIPS data on behalf of the clinician • View all data submitted by/on behalf of the clinician **Note:** There must be a user with the Individual Practitioner role before a user can request the Individual Practitioner Representative role

Who?	EIDM Role	EIDM Role Type	Functions
Groups, including: • **MIPS APM participants** • **Non-QP Advanced APM participants** *(2+ clinicians billing under the TIN)*	**Security Official**	Provider Approver	• Approve "PQRS Submitter" or "Web Interface Submitter" role requests by EIDM account holders for their organization (including EHR/Health IT Vendors reporting on behalf of their TIN) • Submit any MIPS data on behalf of the group, either reporting as a group or for eligible clinicians reporting individually • View all data (including PII) submitted by/on behalf of a group reporting as a group (TIN level) • View all data submitted by/on behalf of the clinicians in the practice reporting individually • Access MIPS performance feedback and payment adjustment information • Submit a targeted review request on qpp.cms.gov • Complete, modify or cancel a registration for the CMS Web Interface and/or CAHPS for MIPS survey
	PQRS Submitter	PQRS Provider	• Submit any non-CMS Web Interface MIPS data

Who?	EIDM Role	EIDM Role Type	Functions
			on behalf of the practice, either as a group or for eligible clinicians reporting individually • View all data (including PII) submitted by/on behalf of the group • Access MIPS performance feedback and payment adjustment information • Submit a targeted review request on qpp.cms.gov • View all data submitted by/on behalf of the clinicians in the practice reporting individually **Note:** An organization must have a Security Official before a user can request the PQRS Submitter role
	Web Interface Submitter	PQRS Provider	• Submit CMS Web Interface MIPS data on behalf of the practice • View all data (including PII) submitted by/on behalf of the practice • View all data submitted by/on behalf of the clinicians in the practice reporting individually • Access MIPS performance feedback and payment adjustment information

Who?	EIDM Role	EIDM Role Type	Functions
			• Submit a targeted review request on qpp.cms.gov **Note:** An organization must have a Security Official before a user can request the Web Interface Submitter role
Individual/Solo Practitioners, including • **MIPS APM participants** • **Non-QP Advanced APM participants** *(1 clinician billing under the TIN/SSN)*	**Individual Practitioner**	Provider Approver	• Approve "PQRS Submitter" role requests by EIDM account holders for the clinician (including EHR/Health IT Vendors reporting on behalf of the clinician) • Submit data on behalf of the clinician • Access MIPS performance feedback and payment adjustment information • Submit a targeted review request on qpp.cms.gov • View all data submitted by/on behalf of the clinician
	Individual Practitioner Representative	PQRS Provider	• Submit any MIPS data on behalf of the clinician • View all data submitted by/on behalf of the clinician • Access MIPS performance feedback and payment adjustment information

Who?	EIDM Role	EIDM Role Type	Functions
			• Submit a targeted review request on qpp.cms.gov **Note:** There must be a user with the Individual Practitioner role before a user can request the Individual Practitioner Representative role
Qualified Clinical Data Registries (QCDRs) **Qualified Registries**	**Security Official**	Provider Approver	• Approve "PQRS Submitter" role requests by EIDM account holders under the TIN • Submit data on behalf of a group/ clinician • View the data they submitted on behalf of the group/ clinician
	PQRS Submitter	PQRS Provider	• Submit data on behalf of a group/ clinician • View the data they submitted on behalf of the group/ clinician **Note:** An organization must have a Security Official before a user can request the PQRS Submitter role
EHR/Health IT Vendors	**PQRS Submitter**	PQRS Provider	• Submit MIPS data on behalf of the group/clinician • View all data submitted by/on behalf of the group/clinician ***IMPORTANT*** EHR/Health IT Vendors must request this

Who?	EIDM Role	EIDM Role Type	Functions
			role for **each** group or individual practitioner for whom they are submitting data. (One request per TIN.) Please note that these groups and/or individual practitioners must have an EIDM account with the appropriate Provider Approver role to approve the EHR/Health IT Vendor role request.

IV. What Do I Do Now?

- **Determine whether your organization is already registered in EIDM**

  To find out if your practice or organization is already registered in the EIDM, please contact the Quality Payment Program by phone at 1-866-288-8292 / TTY 877-715-6222 or by email at qpp@cms.hhs.gov. You will need to provide the group's TIN and the name of the group.

- **Identify your organization's Security Official**

  To determine the group's Security Official, please contact the Quality Payment Program by phone at 1-866-288-8292 / TTY 877-715-6222 or by email at qpp@cms.hhs.gov. You will need to provide the group's TIN and the name of the group.

  If your group does not already have a Security Official, designate one.

- **Gather the required information for each role**
  - Users requesting the **Security Official** role must provide:
    - Group's Medicare billing TIN,
    - Legal Business Name,
    - Rendering NPIs for **two different** eligible clinicians who bill under the TIN and their corresponding individual Provider Transaction Access Numbers (PTANs) (do not use the GROUP NPI or GROUP PTAN), and
    - Organization Address, City, State, Zip Code, and Phone Number.
  - Users requesting the **Individual Practitioner** role must provide:

- Clinician's Name,
- Clinician's Medicare billing TIN,
- Legal Business Name,
- Clinician's Rendering NPI and corresponding individual Provider Transaction Access Numbers (PTAN), and
- Address, City, State, Zip Code, and Phone Number.

- Users requesting the **PQRS Submitter, Web Interface Submitter, or Individual Practitioner Representative** role must provide:
  - Group's Medicare billing TIN,
  - Legal Business Name, and
  - Address, City, State, Zip Code, and Phone Number.

Review the HHS Rules of Behavior, which govern the use of systems containing Personally Identifiable Information (PII) and Personal Health Information (PHI)

- These rules, which include prohibitions against unauthorized access (such as sharing account information), are located here: https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/rules-of-behavior-for-use-of-hhs-information-resources/index.html
- Please note that when creating an EIDM account or requesting an EIDM role, you will be required to acknowledge your agreement to abide by these rules

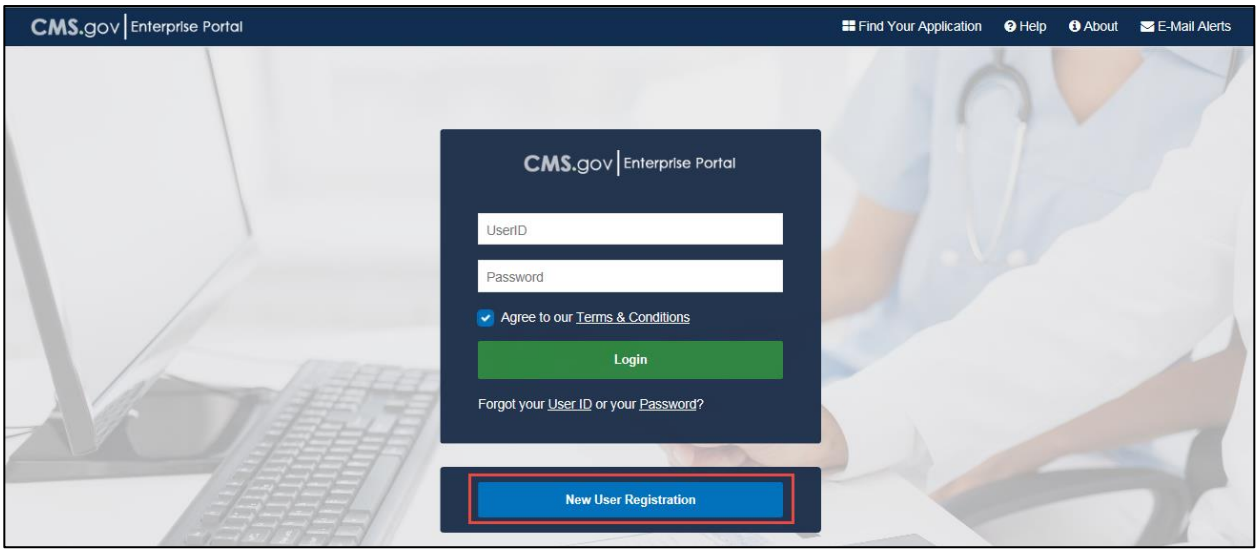
Create an EIDM account and/or request the appropriate role by following the instructions in this guide

Note: You have **twenty-five (25)** minutes to complete each screen (unless a different time is noted on the screen). If you take longer than 25 minutes to complete a screen, you will lose all the information you entered and will need to start the process again.

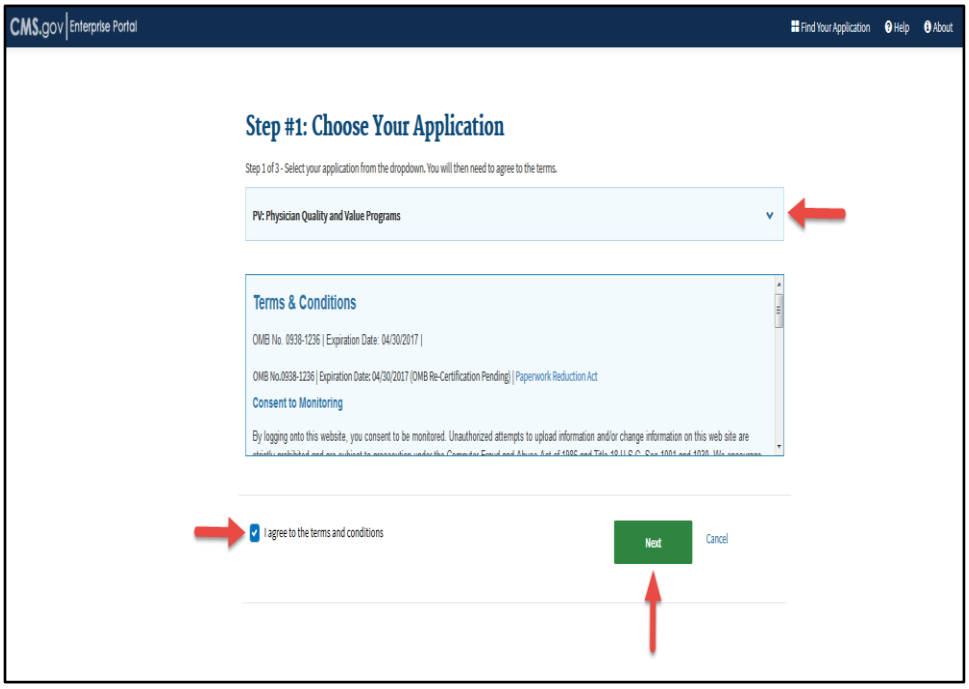
V. Creating an EIDM Account

Already have an EIDM Account? Skip this section.

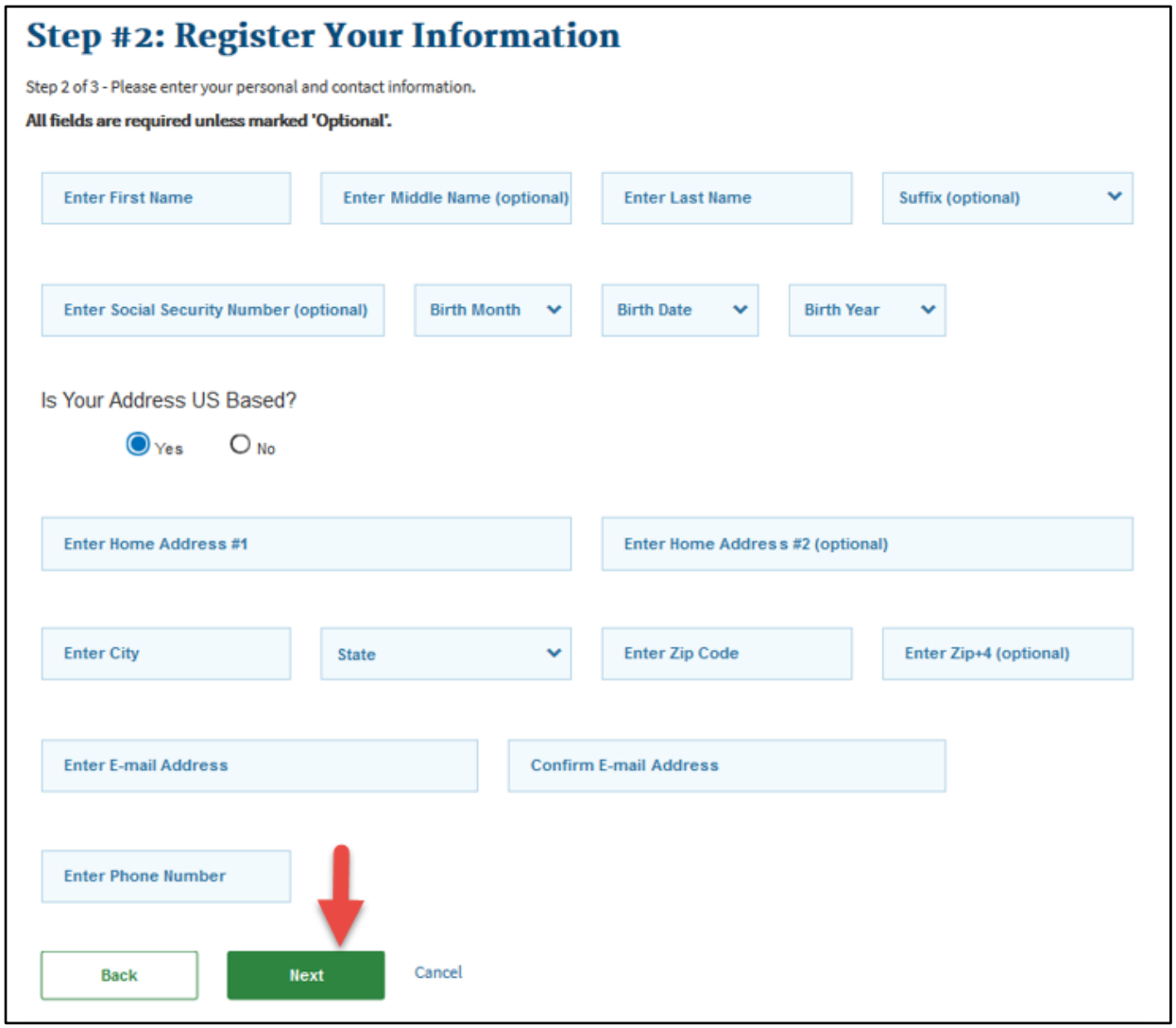
1. Navigate to https://portal.cms.gov/. The CMS Enterprise Portal page is displayed.
2. Select the '**New User Registration'** link.



3. Select **PV: Physician Quality and Value Programs** from the drop-down list, select '**I agree to the terms and conditions**,' and then select '**Next**' to continue with the registration process.



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 must 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 your EIDM User ID and Password of your choice and based on the requirements for creating a user ID.

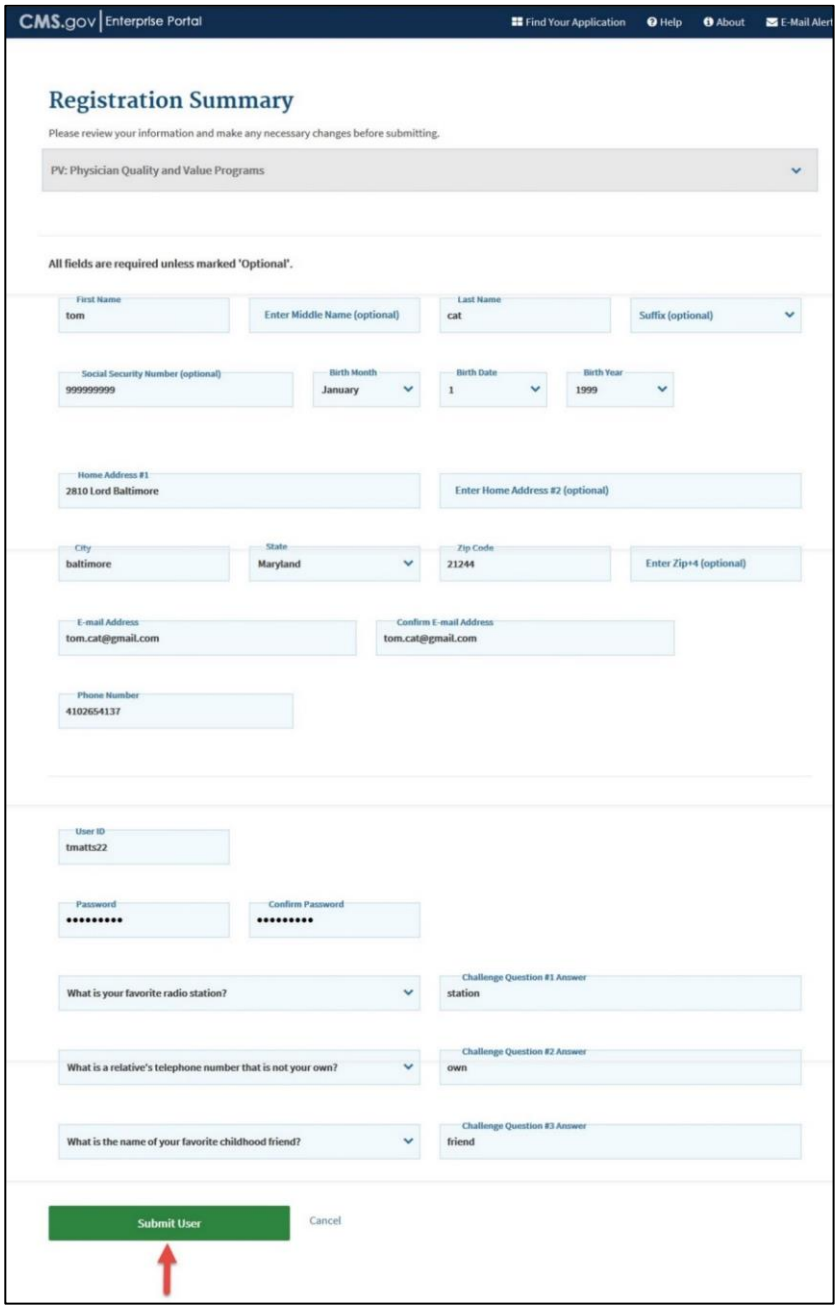
   Note: Your **EIDM User ID** must be a minimum of six (6) and a maximum of seventy-four (74) alphanumeric characters. It must contain at least 1 letter and cannot contain your Social Security Number or any 9 consecutive numbers. Allowed special characters are dashes (-), underscores (_), apostrophes ('), and periods (.) followed by alphanumeric characters.

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

   Note: Your **EIDM Password** must be a minimum of eight (8) and a maximum of twenty (20) characters in length. It must contain at least one (1) letter, one (1) number, one (1) uppercase letter, and one (1) lowercase letter. It cannot contain your User ID and the following special characters may not be used: ?, <, >, ( ), ', ", /, |, and &. Your password must be changed at least every 60 days and can only be changed once a day.

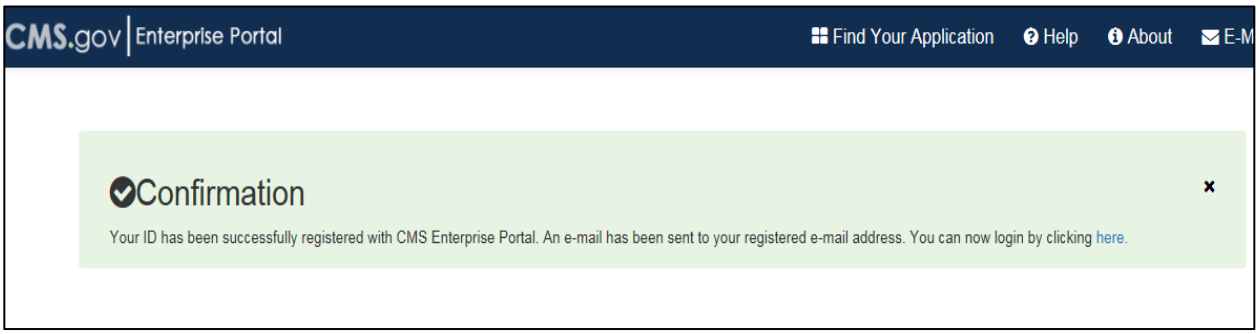
6. **Select three (3) security questions** from the Security Question drop-down menu and provide the answer to each security questions.
7. Select **Next.**

Review the **Registration Summary** screen and select **Submit User** to continue with the new registration process.



Your registration for an EIDM account is now complete. You will receive an E-mail acknowledging your successful account creation with your EIDM User ID.

You can login to the CMS Enterprise Portal by clicking on the “here” link.



VI. Requesting an Approver Role

Skip this section if you:

- Are an EHR/Health IT Vendor that is not a CMS-approved Qualified Clinical Data Registry or Qualified Registry
- Already have a Provider Approver for your organization

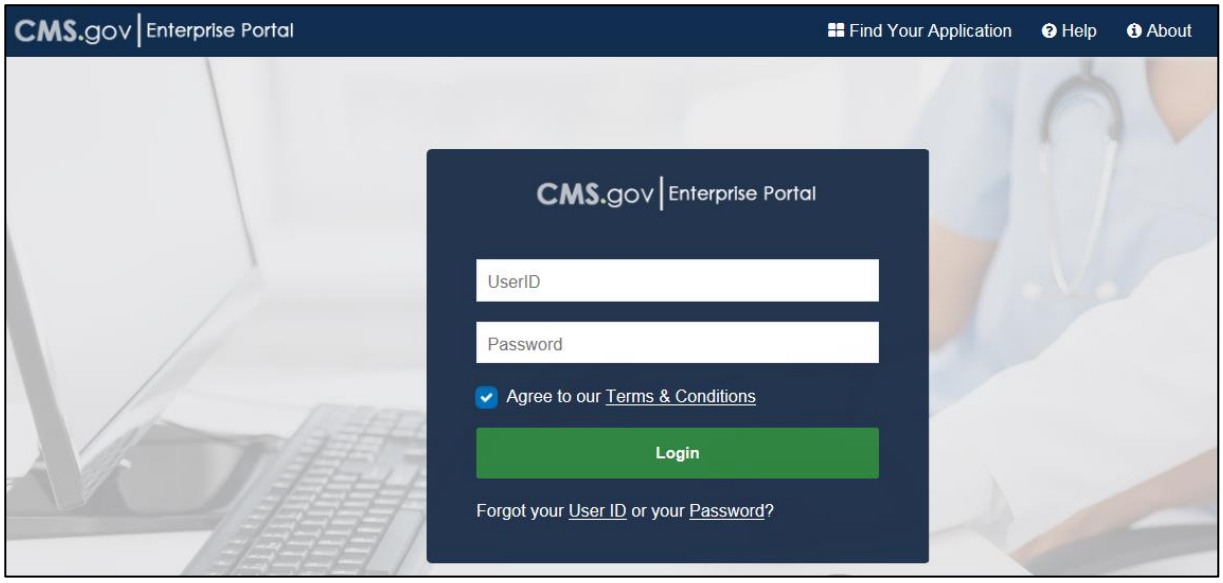
PLEASE NOTE: A ‘Provider Approver’ role is the first role that must be requested by an organization/individual practitioner, because the user with this role will approve all subsequent role requests for the organization/individual practitioner.

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 qpp@cms.hhs.gov for assistance.

The section provides instruction for users for requesting the following Provider Approver roles:

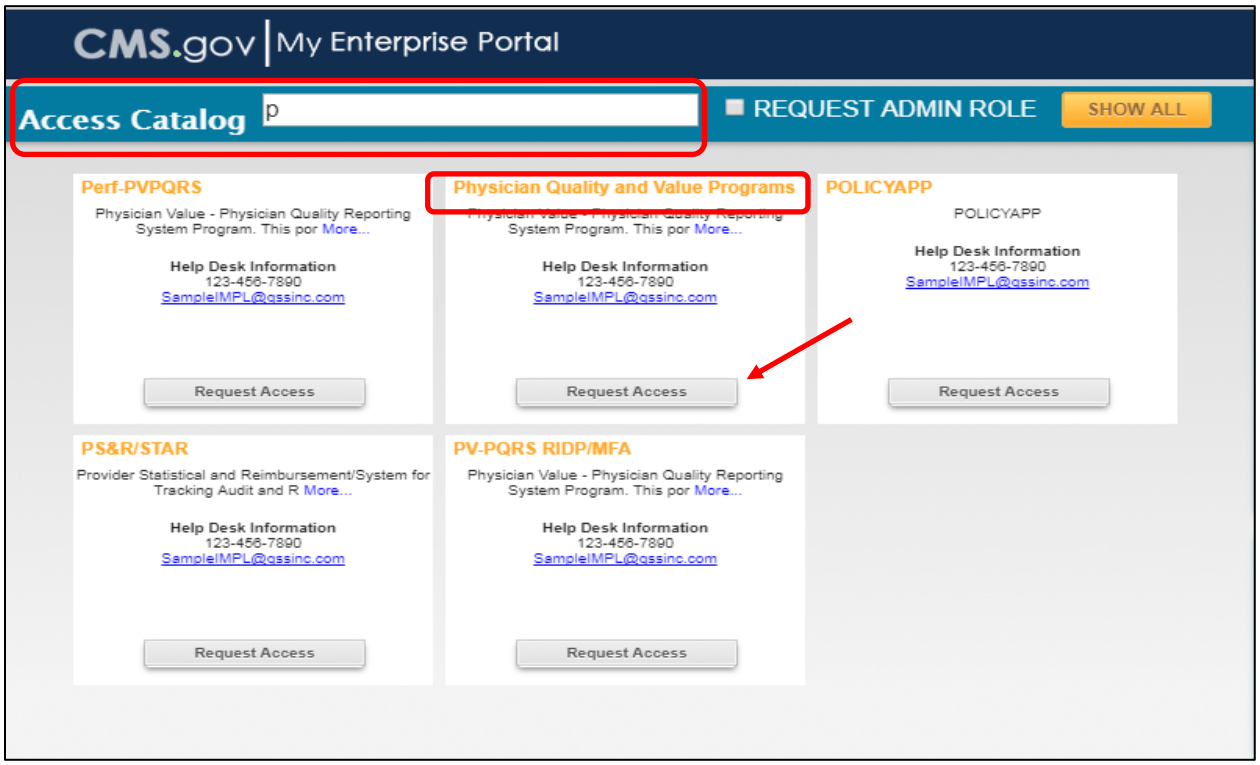
- **Security Official** (Groups with 2+ clinicians, CPC+ Practice Sites, Qualified Registries, Qualified Clinical Data Registries)
- **Individual Practitioner** (1 clinician billing under the TIN/SSN)

1. Navigate to https://portal.cms.gov/. The CMS Enterprise Portal home page is displayed.
2. Once on the page, enter your EIDM **user ID** and **password**. **Select Agree to our Terms & Conditions** checkbox and then select **Login** on the CMS Enterprise Portal.



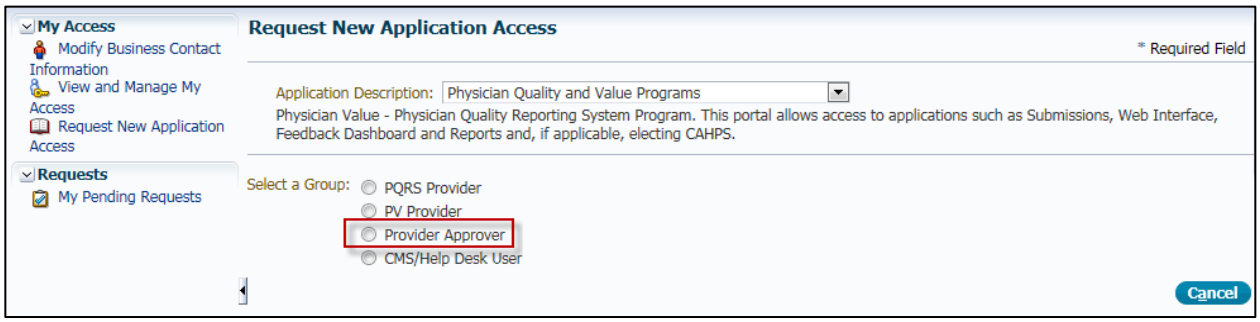
3. Upon initial login, the CMS Enterprise Portal My Portal page is displayed. Select Request/Add Apps link on the My Portal screen page to begin the process of requesting a new user role request access to CMS Systems/Applications

4. Select the '**Physician Quality and Value Programs'** domain and select '**Request Access.'**



Note: The Access Catalog list presented is in alphabetical order. Scroll down until you find the Physician Quality and Value Programs application or enter the first few letters of the application in the Access Catalog text box to narrow down the selection criteria.

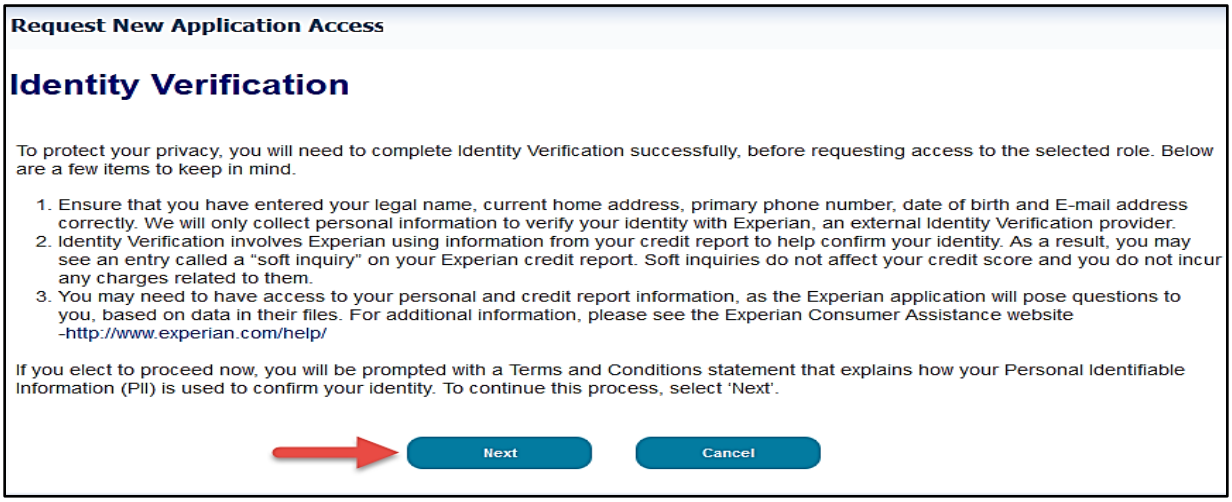
5. At the top of the next screen, the Physician Quality and Value Programs application will be auto-populated. Under '**Select a Group'**, select ''



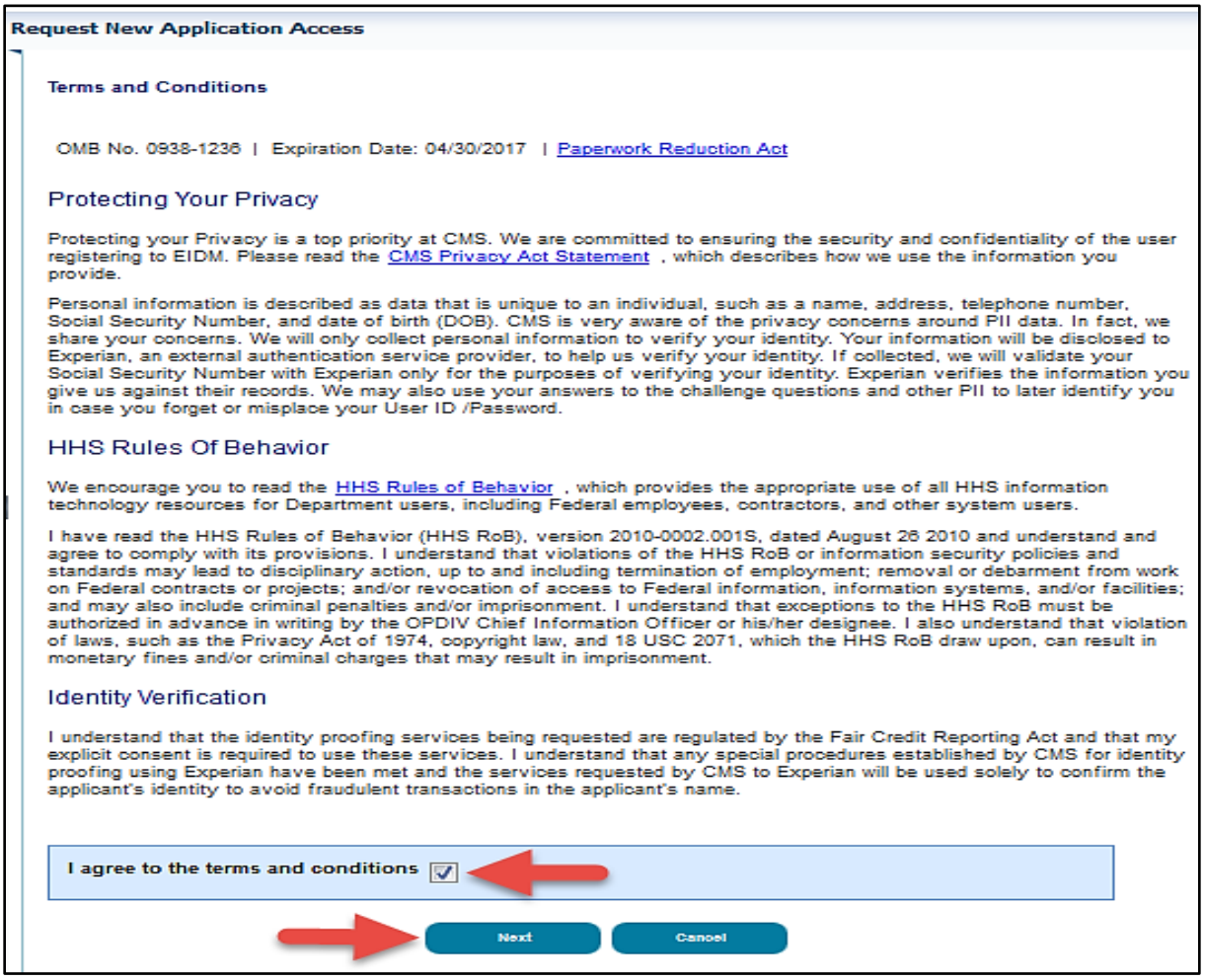
6. Select the appropriate '**Approver Role'**, either '**Security Official'** or '**Individual Practitioner'**, then select '**Next**'.

   NOTE: The '**Security Official'** role will be selected for those users in a third-party organization or that have multiple eligible clinicians (2+) billing under a TIN. The '**Individual Practitioner**' role will be selected for those that are a sole proprietor billing under a TIN or SSN.

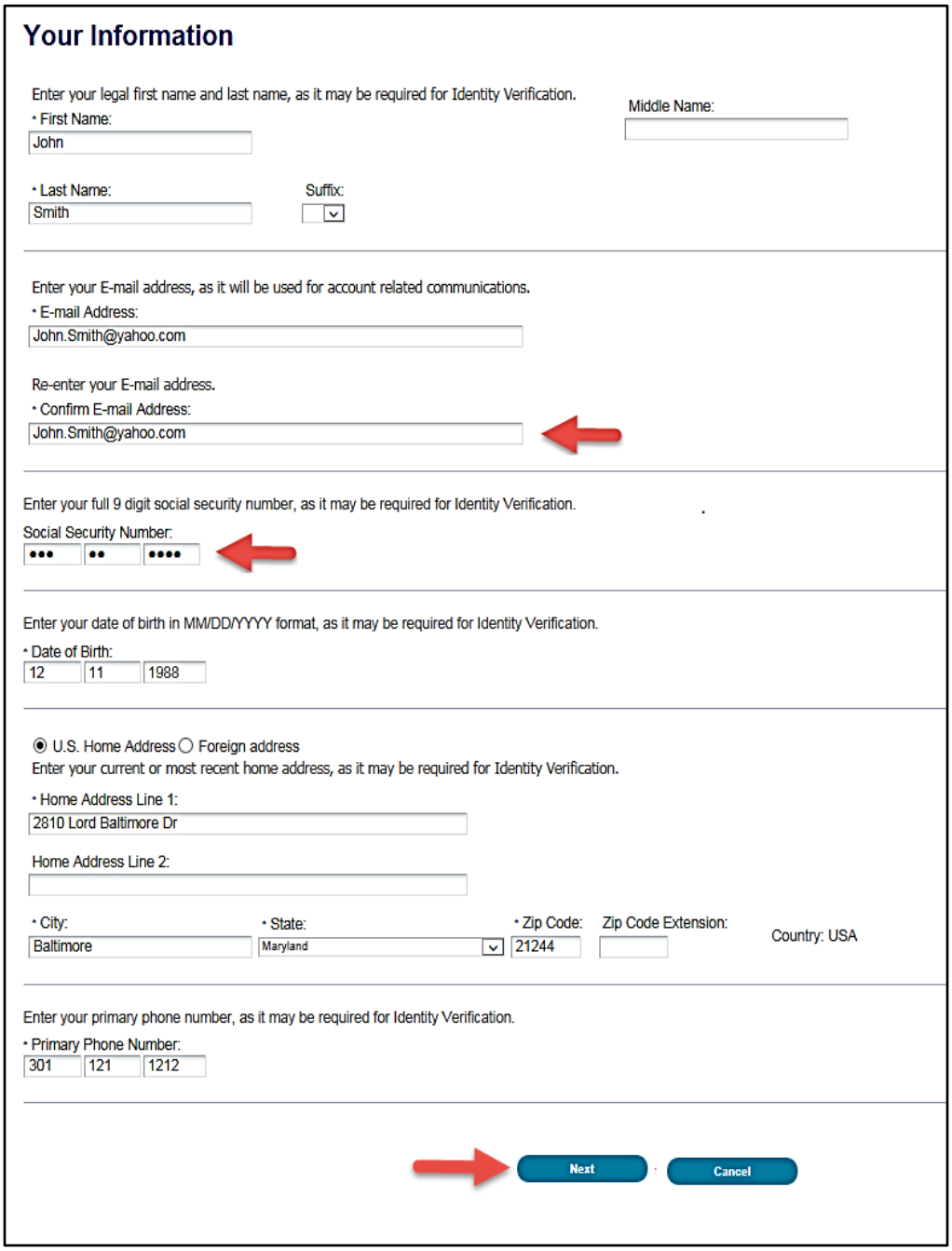
7. Select '**Next**' to complete the '**Identity Verification'** section. The Identity Verification process will only be completed the first time a user requests a role in the Physician Quality and Value Programs domain in EIDM. If the Identity Verification has been completed, users can skip to step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



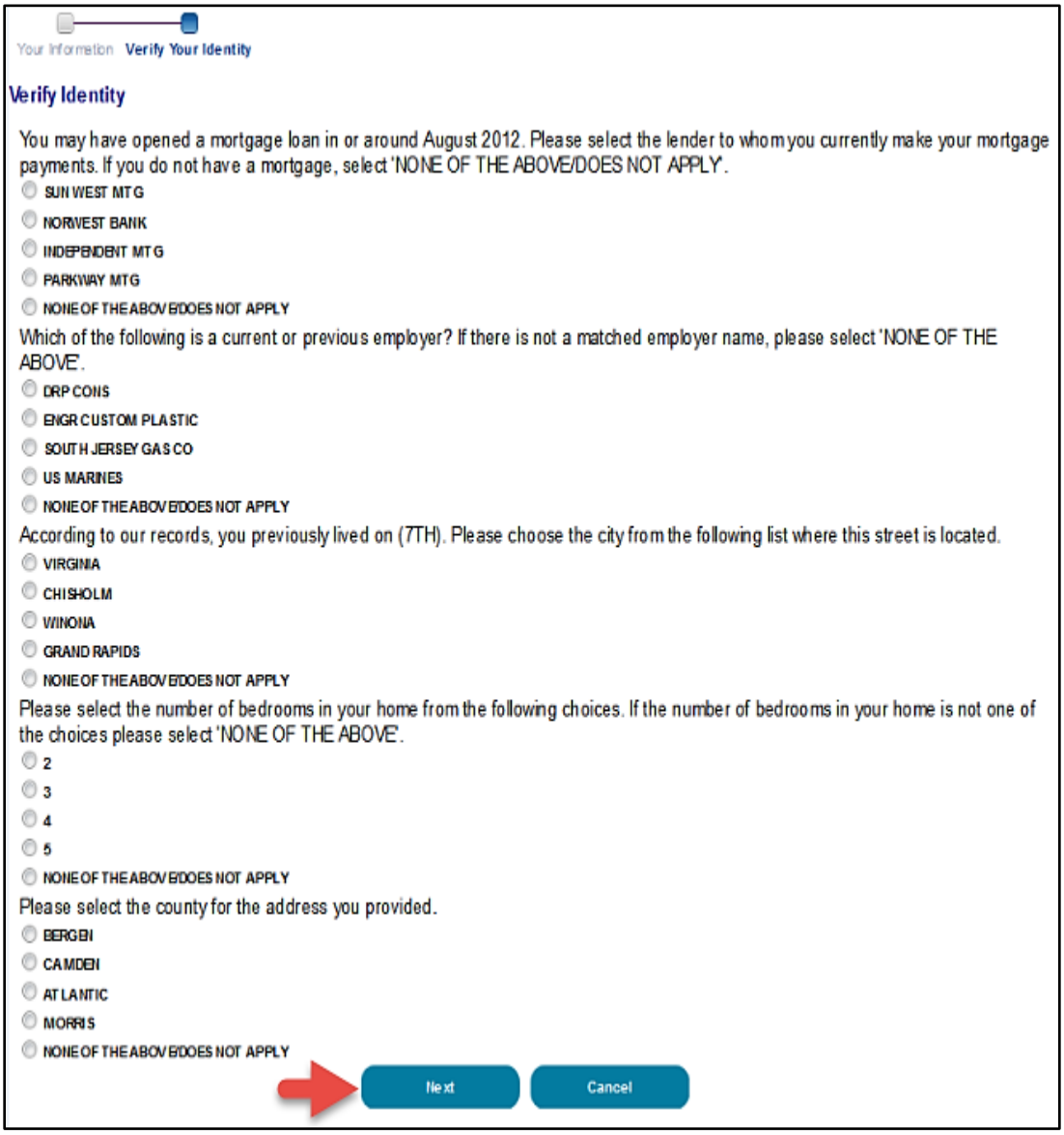
8. Read the Terms and Conditions. Select the '**I agree to the terms and conditions'** checkbox and then select '**Next**', which will be enabled only after checking the '**I agree to the terms and conditions**' checkbox.



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

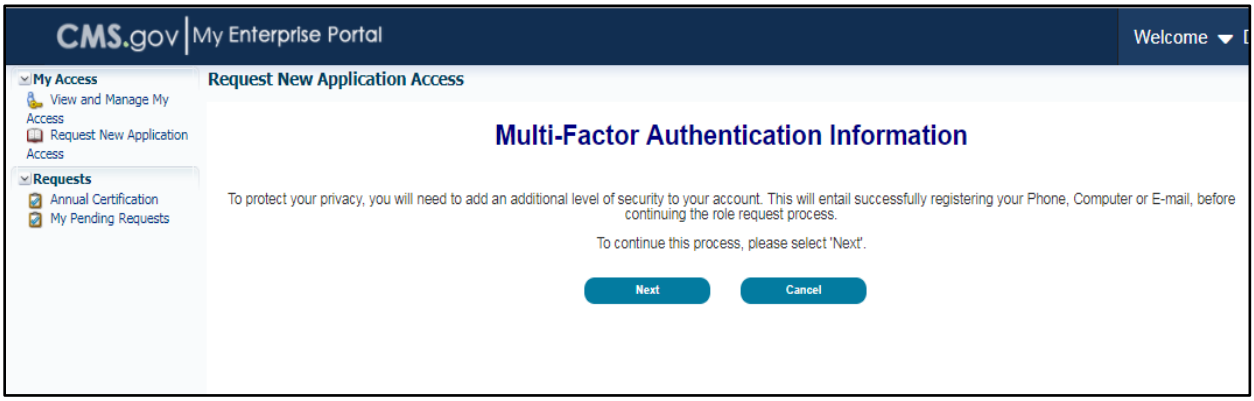


10. Select an answer to each question under '**Verify Identity'**. Select '**Next**' after providing an answer to each question. '**Verify Identity'** question information is provided from Experian in association with the SSN Number provided in step 10.

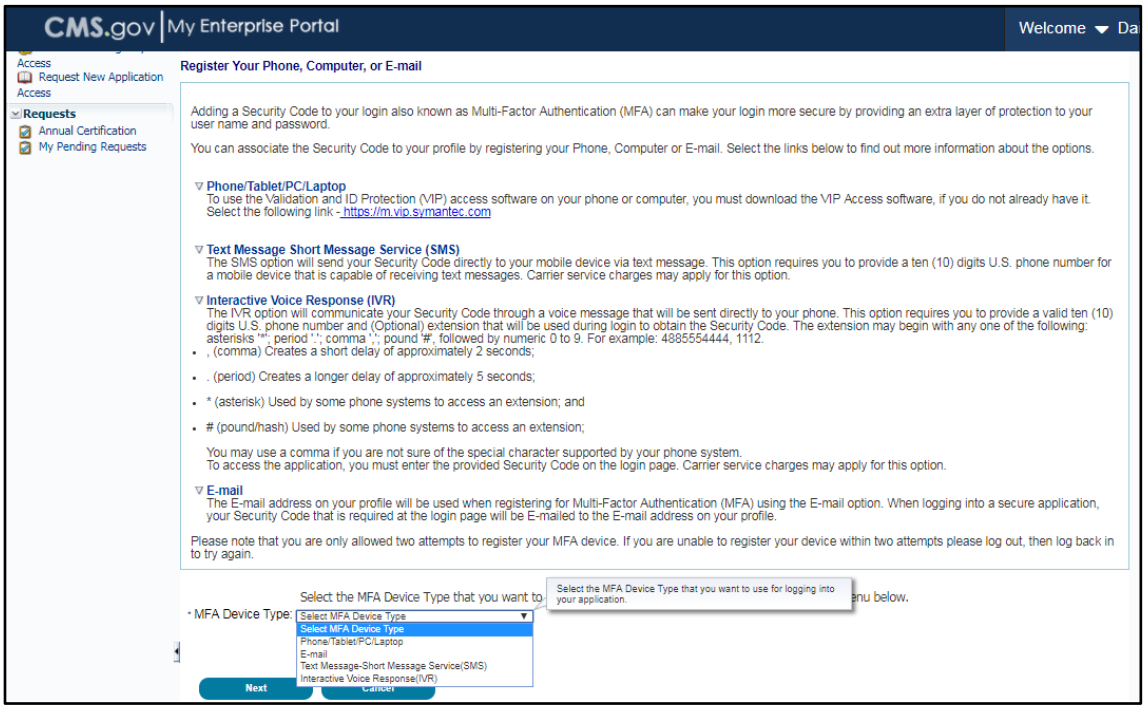


11. Remote Identity Proofing is now complete. Select '**Next'** to proceed to the 'Multi-Factor Authentication Registration' process.

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 '**MFA Device 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 (https://vip.symantec.com/). If the VIP Access Software is not installed on your device, you will be unable to complete the Multi-Factor Authentication process.

    - Credential ID
    - MFA Device Description

    (b) If selecting **E-mail One Time Password (OTP)** as Credential Type, the E-mail address on your profile will automatically be used for the E-mail option to obtain the security code and the following required information fields will be displayed:

    - MFA Device Description

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

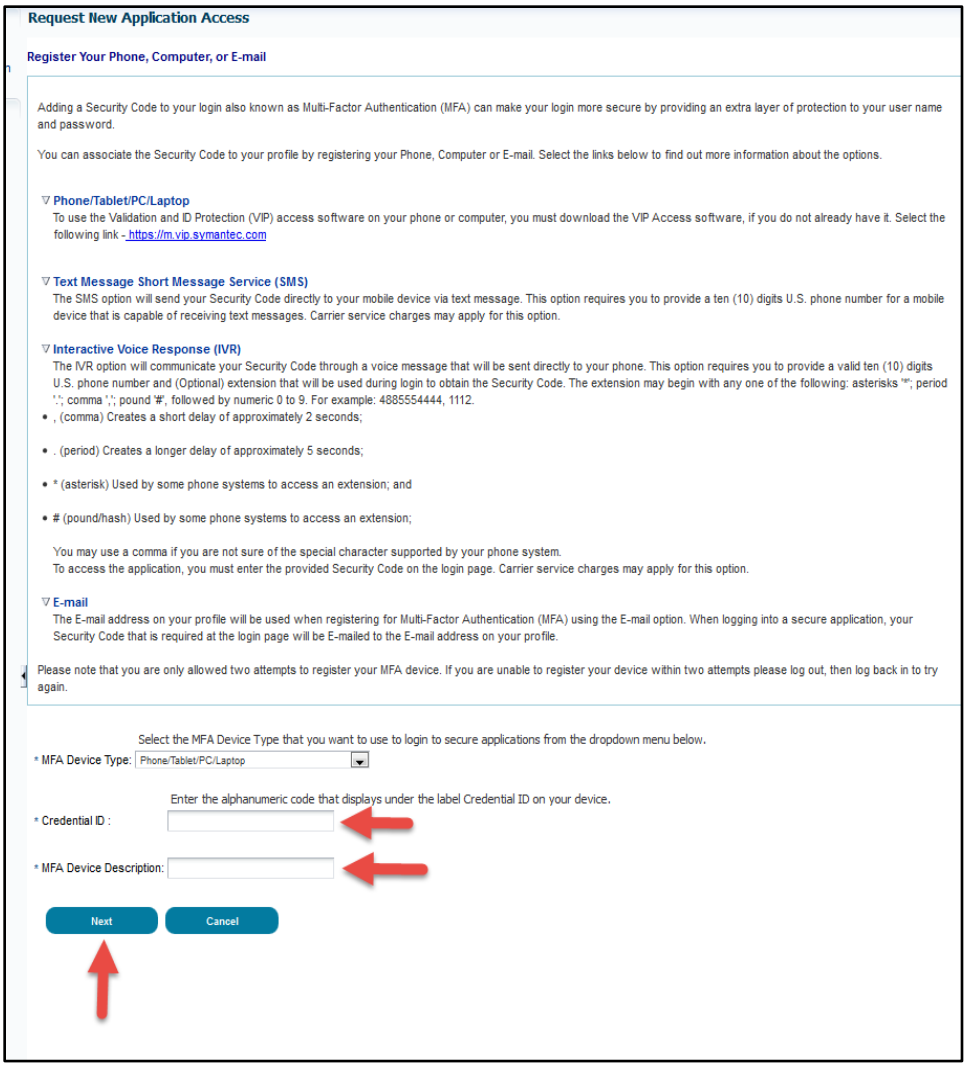
    - Phone Number
    - MFA Device Description

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

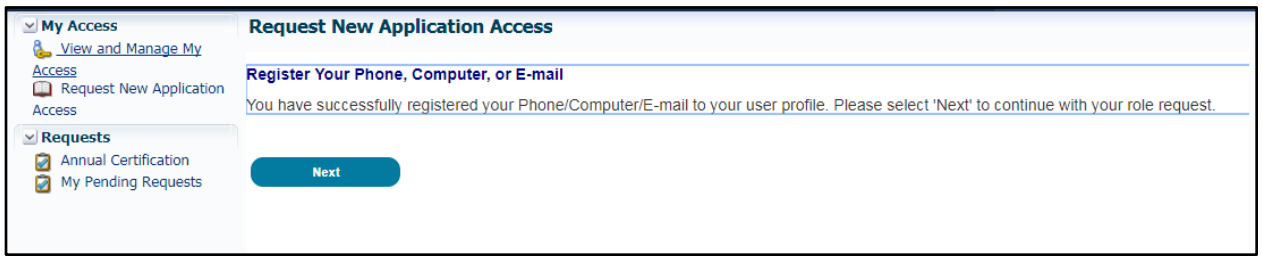
    - Phone Number and Extension
    - MFA Device Description

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

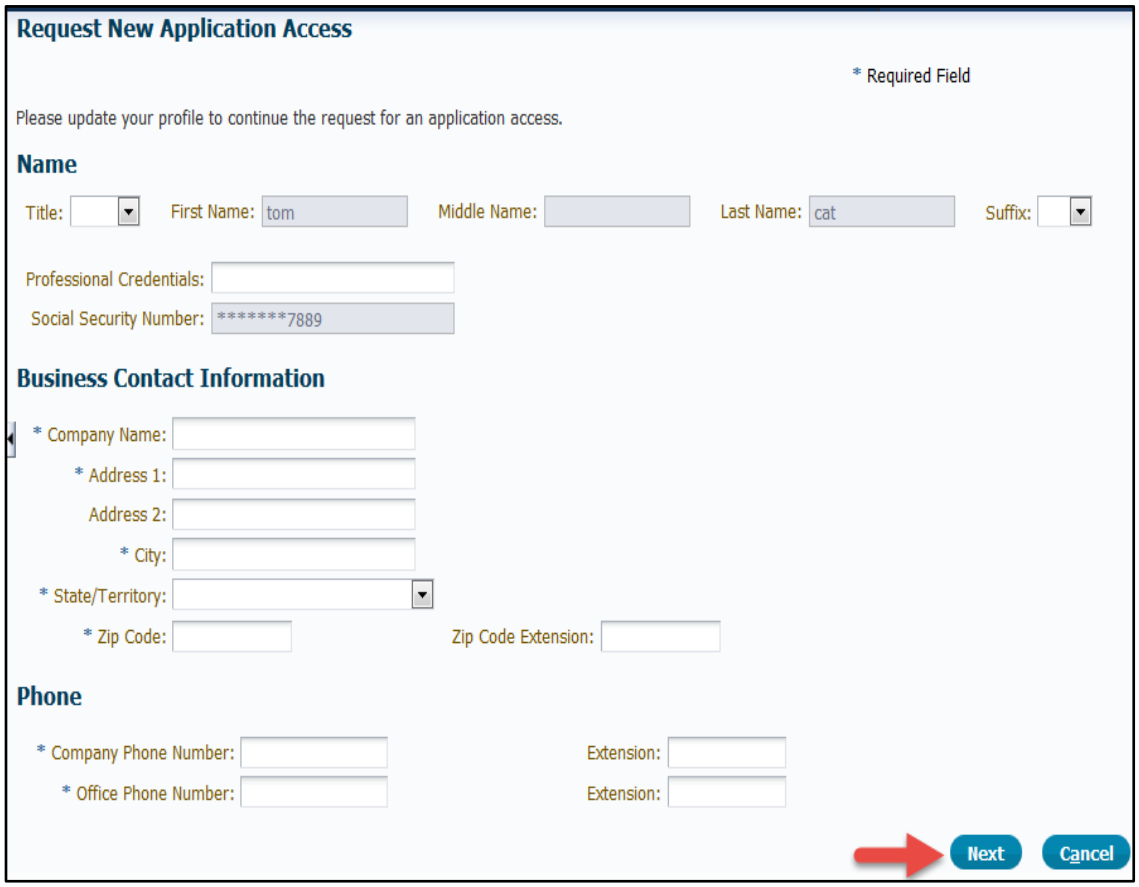
(Screen shot on next page)


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

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



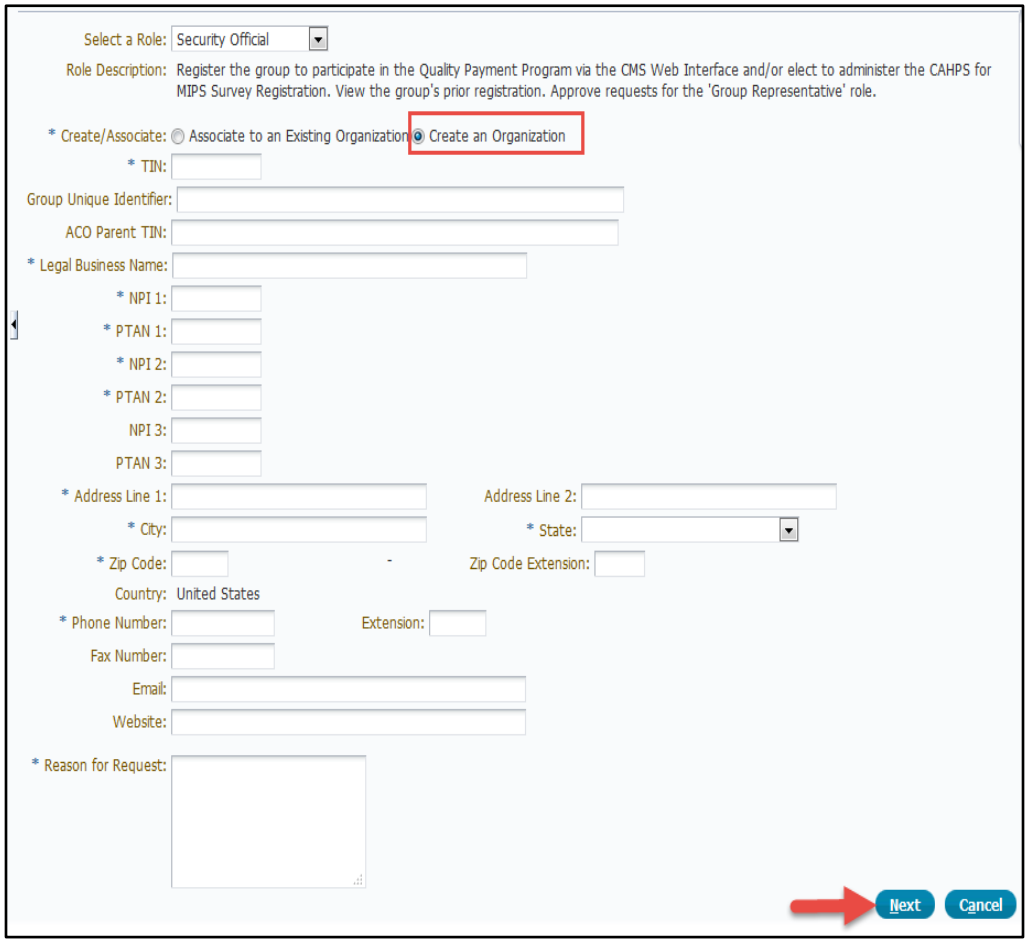
16. On the **Request New Application Access** page, provide the required information under the **Business Contact Information** and **Phone** sections. Note that the information in the Name section will be pre-populated with the Remote Identity Proofing information.



17. Refer to step **17A** for information on requesting a '**Security Official'** role and **17B** for information on requesting an '**Individual Practitioner'** role.

A. Security Official (SO)

- Select either '**Create an Organization'** or '**Associate to an Existing Organization'**
- The first user registering on behalf of the organization will select **'Create an Organization'**; other users registering with an existing EIDM organization will select '**Associate to an Existing Organization'**.
  - To **Create an Organization:**
    - Complete the required information for the practice and select **Next** to continue



NOTE: When creating a new organization, you have 3 attempts to enter 2 valid individual National Provider Identifier/Provider Transaction Account Number (NPI/PTAN) combinations. If the information is a confirmed match, the request will be auto approved. If you exceed these attempts, your request will be sent on for manual approval.

Example: Healthy Clinic with Medicare billing TIN 11-1111111 has ten eligible professionals in the group. Enter the rendering NPI and individual PTAN combinations for two of the eligible clinicians: Dr. Smith and Dr. Beaver.

- Dr. Smith's rendering NPI is 4545454545 and the corresponding individual PTAN is G676767676.

Note: PTANs are alphanumeric therefore, enter the alpha characters.

- Dr. Beaver's rendering NPI is 2525252525 and the corresponding individual PTAN is 0012789456.

Note: All leading zeroes in the PTAN should be entered.

***Registries and QCDRs:** Qualified Registries and Qualified Clinical Data Registries have no NPI/PTAN combinations associated with their Tax ID and will have to be manually approved. Please enter all 0s (zeroes)_in these fields; after the 3rd failed attempt, your request will be routed to the Quality Payment Program for manual approval.

ii. To **Associate to an Existing Organization**

a. Enter one of the following for your practice:

- Medicare Billing TIN (preferred search criteria)

OR

- Legal Business Name and State

OR

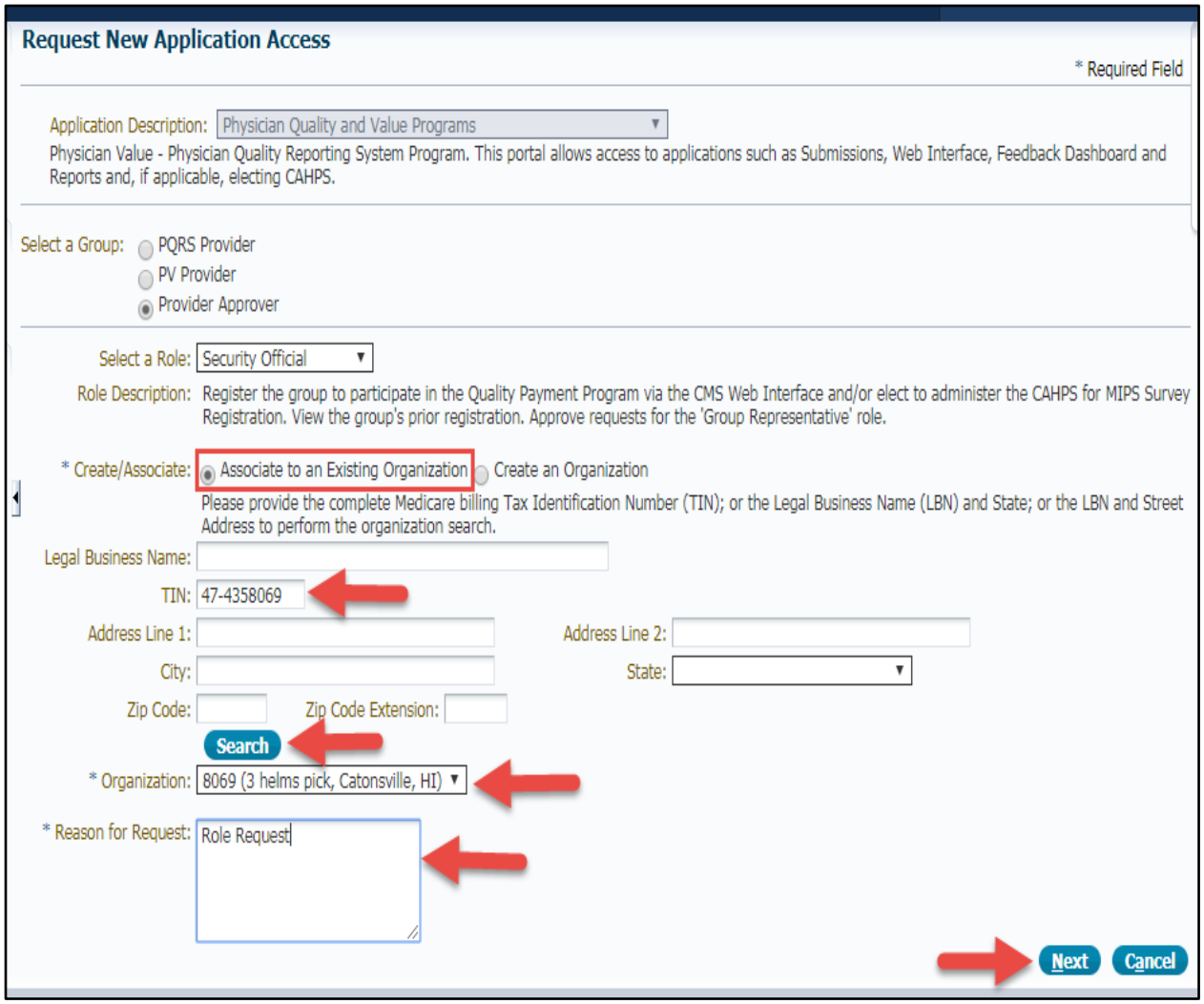
- Legal Business Name and Street Address

b. Select **Search**

c. Select your group practice from the **Organization** drop-down menu.

d. Enter **Reason for Request** and select **Next**.

Note: If your group practice cannot be found, please verify that your group practice already has a user with an approved Security Official role and you entered the group practice's Medicare billing TIN correctly. Contact the Quality Payment Program for assistance.



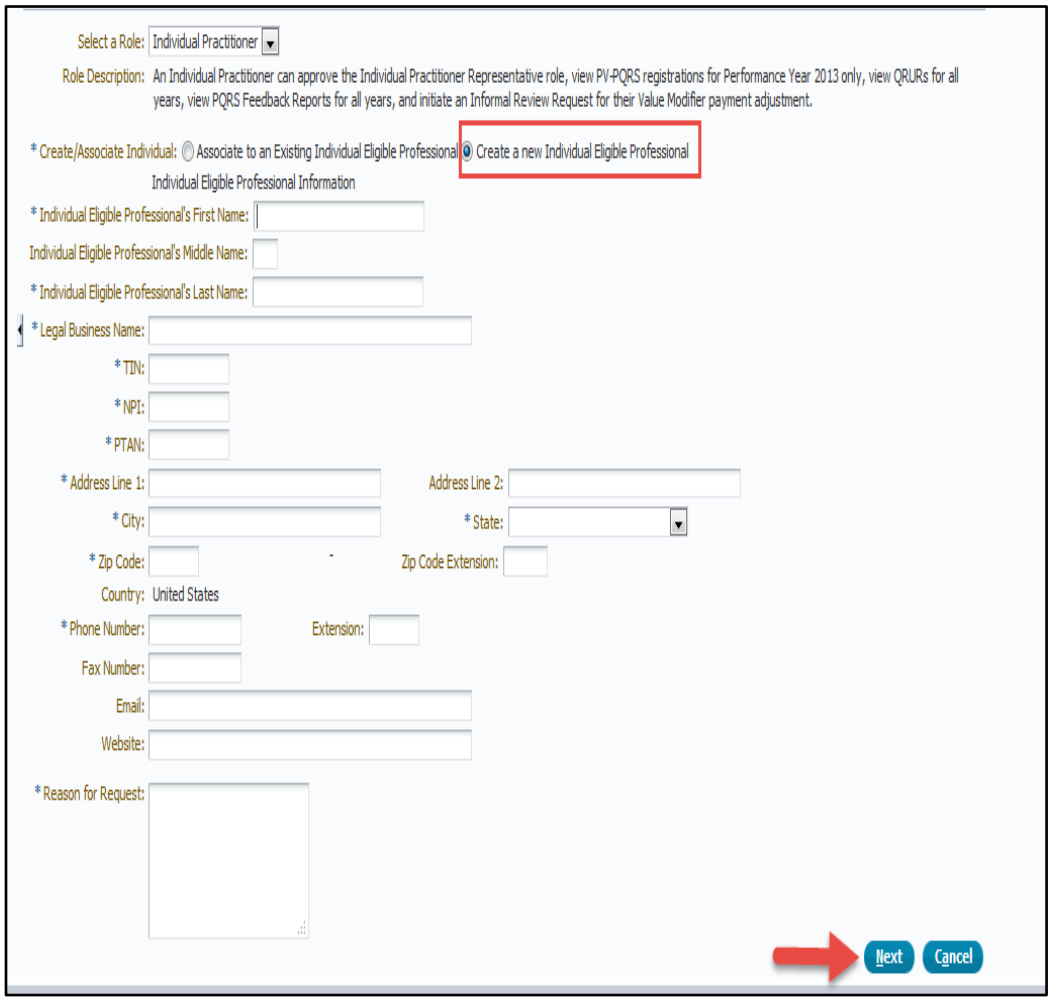
NOTE: When associating to an existing organization, the request will be sent to the Security Official for approval.

B. Individual Practitioner (IP)

- Select either ‘Create a New Individual Eligible Professional’ or ‘Associate to an Existing Individual Eligible Professional’
- The first user registering on behalf of the Individual Practitioner will select ‘Create a New Individual Eligible Professional’; other users registering with an existing EIDM Individual Practitioner will select ‘Associate to an Existing Individual Eligible Professional’.

  i. To Create a New Individual Eligible Professional

  - Complete the required information for the provider and select Next to continue



NOTE: When creating an Individual Practitioner, you have 3 attempts to enter the valid individual NPI/PTAN combination. If the information is a confirmed match, the request will be auto approved. If you exceed these attempts, your request will be sent on for manual approval. If further assistance is needed, contact the Quality Payment Program.

Example: Dr. Smith's Family Practice with Medicare billing TIN 11-1111111 has a sole eligible clinician in the group. Enter Dr. Smith's rendering NPI and individual PTAN combinations.

- Dr. Smith's rendering NPI is 4545454545 and the corresponding individual PTAN is G676767676.

Note: PTANs are alphanumeric therefore, enter the alpha characters, as well as any leading zeroes in the PTAN.

ii. To **Associate to an Existing Individual Practitioner**

a. Enter one of the following for the provider:

Medicare Billing TIN (preferred search criteria)

OR

Legal Business Name and State

OR

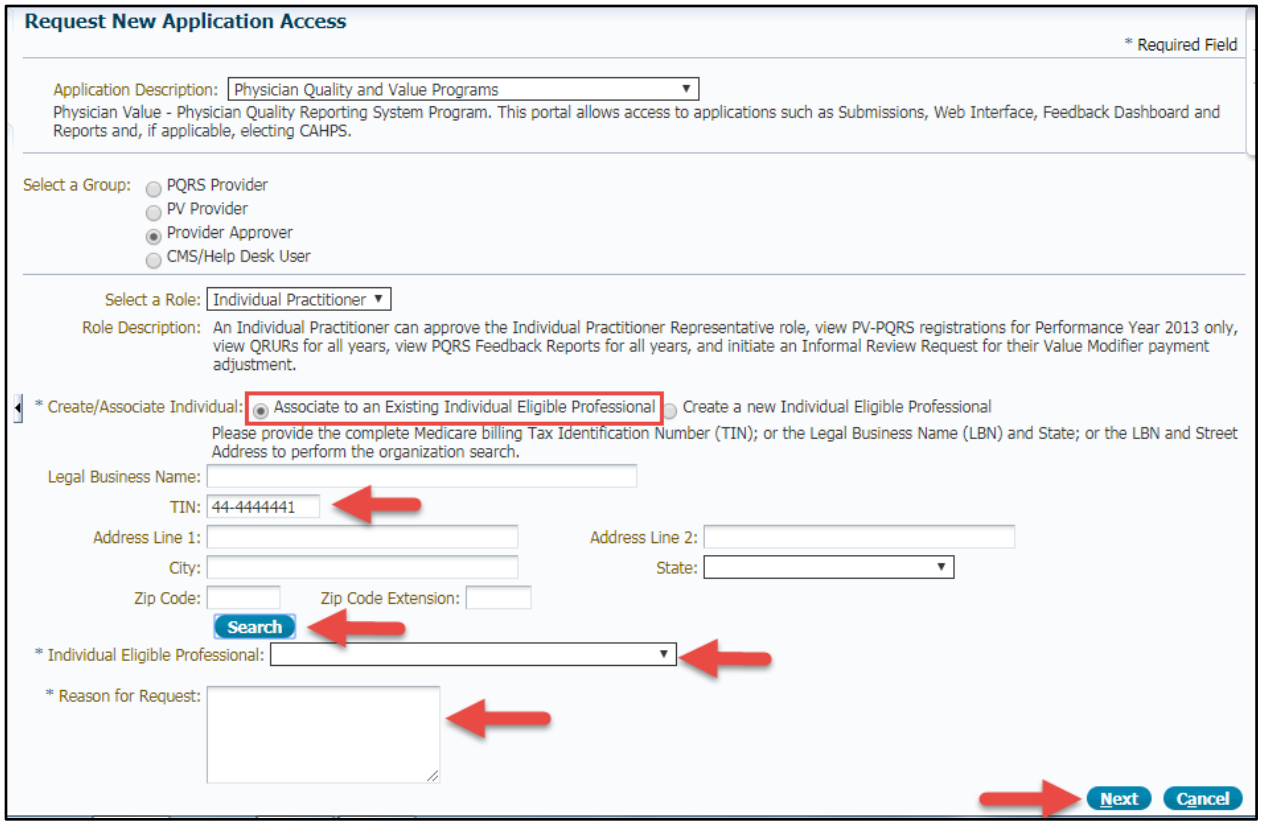
Legal Business Name and Street Address

b. Select **Search**

c. Select your group practice from the **Organization** drop-down menu.

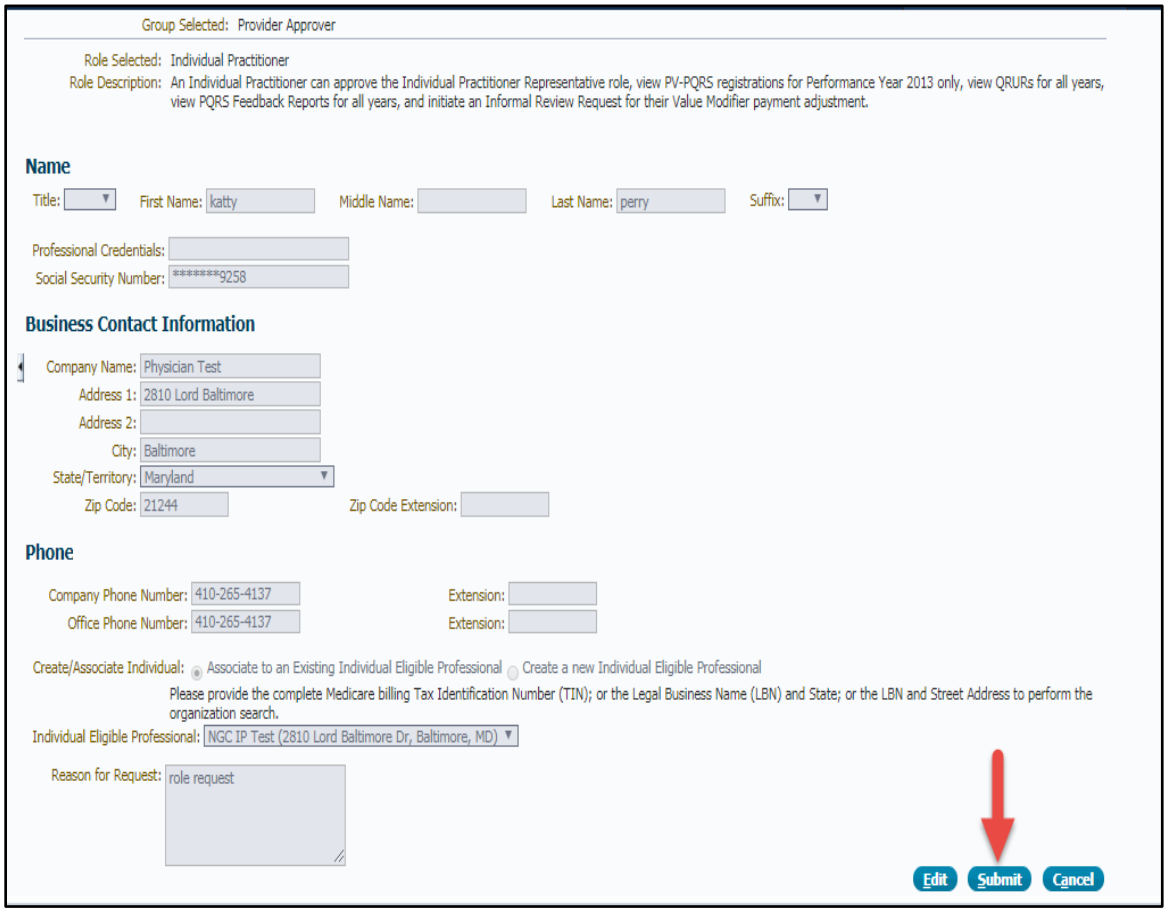
d. Enter Reason for Request and select Next.

Note: If the solo practitioner cannot be found, please verify that the solo practitioner already has a user with an approved Individual Practitioner role and you entered the solo practitioner's Medicare billing TIN correctly. Contact the Quality Payment Program for assistance.

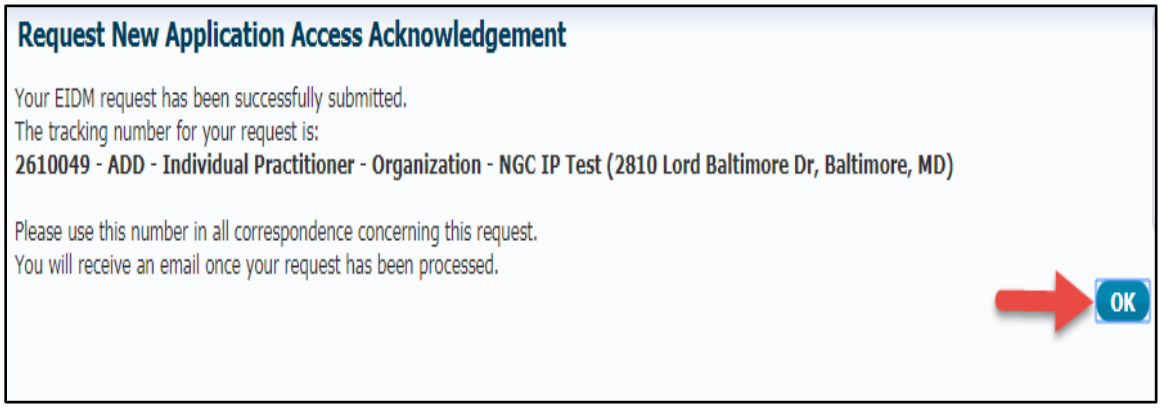


NOTE: When associating to an existing Individual Practitioner, the request will be sent to the Individual Practitioner for approval.

18. Review the entire request to confirm all 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:

- Please be sure to create the new Organization or Individual Practitioner using the provider's(s') Individual NPI and PTAN combination(s). If you need to verify this information, contact your Medicare Part B Contractor.
- 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.

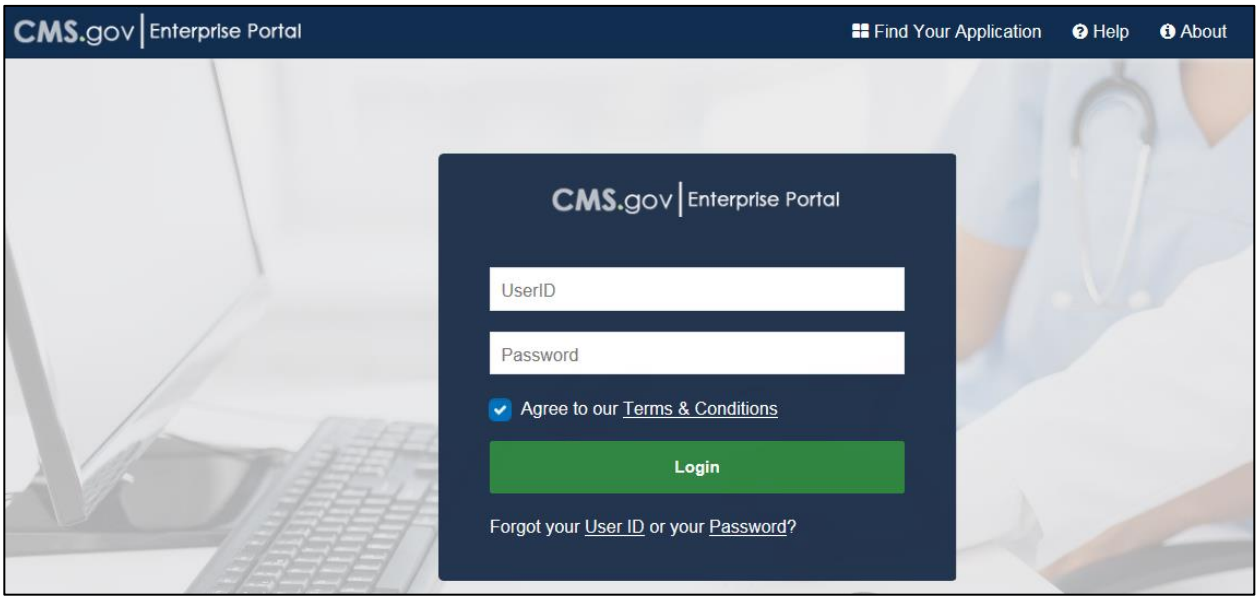
VII. Requesting a Provider Role

Once an organization or individual practitioner has a user with a 'Provider Approver' role, additional users can request roles for the organization.

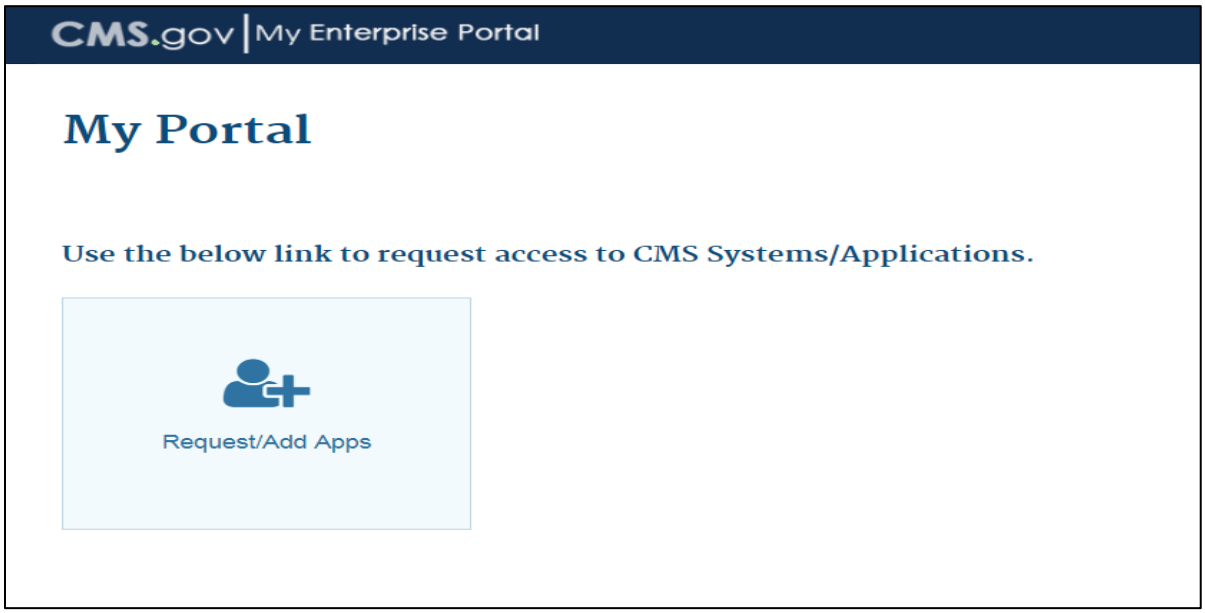
*__IMPORTANT note for EHR/Health IT Vendors__ (that are **not** CMS-approved Qualified Clinical Data Registries or Qualified Registries):__*__ If you are reporting QPP data on behalf of your clients, you will need to repeat these steps for **EACH TIN** ('organization' or 'individual practitioner') for whom you are submitting data.

Please note: Even though the EIDM naming convention still refers to "PQRS", these are the roles needed for QPP submission.

1. Navigate to https://portal.cms.gov. The CMS Enterprise Portal home page is displayed.
2. Once on the page, enter your EIDM **user ID** and **password**. Select **Agree to our Terms & Conditions** checkbox and then select **Login** on the CMS Enterprise Portal.

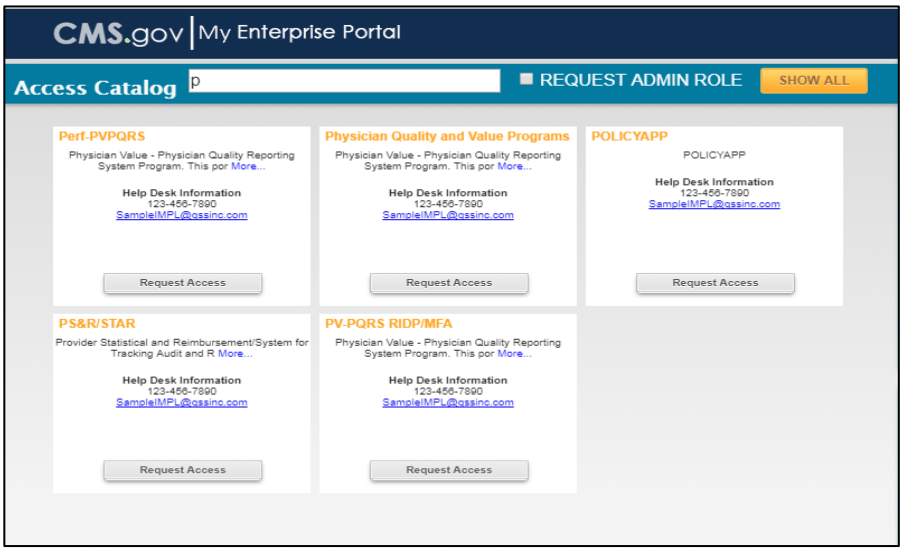


3. Upon initial login, the CMS Enterprise Portal My Portal page is displayed. Select Request/Add Apps link on the My Portal screen page to begin the process of requesting new user role access to CMS Systems/Applications

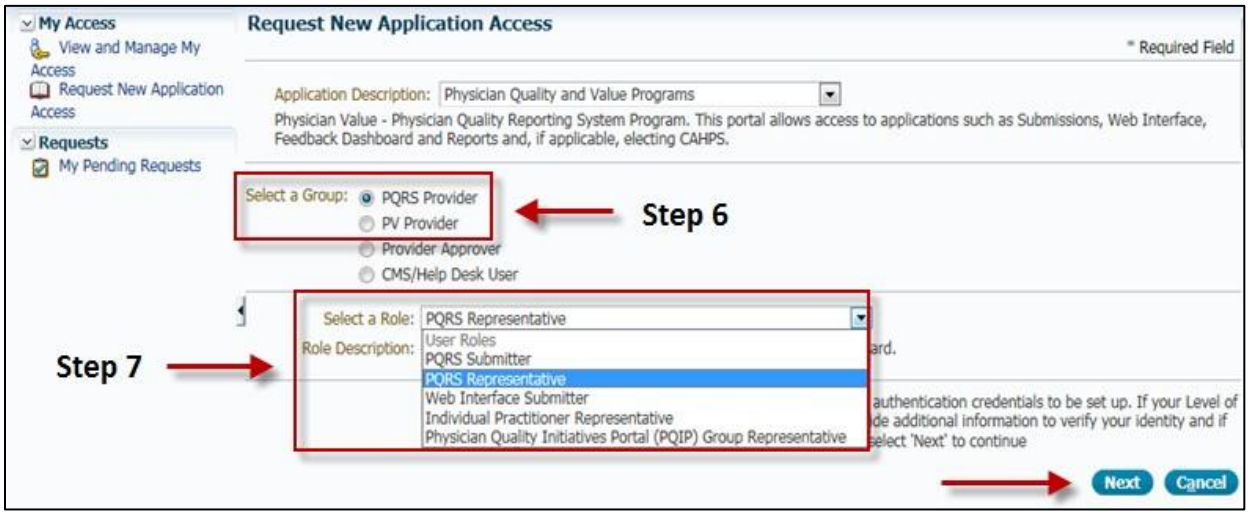


4. Select the 'Physician Quality and Value Programs' domain and select 'Request Access.'

Note: The Access Catalog list presented is in alphabetical order. Scroll down until you find the Physician Quality and Value Programs application or enter the first few letters of the application in the Access Catalog text box to narrow down the selection criteria.

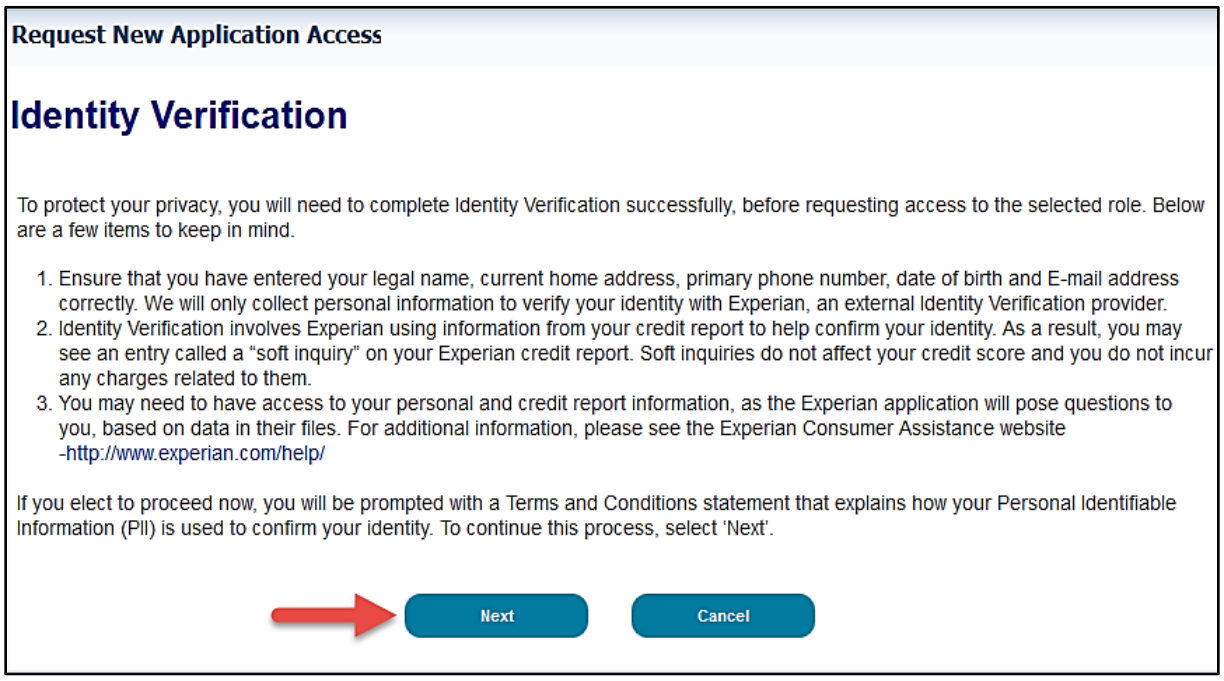


5. The Physician Quality and Value Programs Domain will be auto-populated. Under '**Select a Group'**, select '**PQRS Provider**.'
6. Select the appropriate '**Role**' from the drop-down menu. The roles listed in the beginning of this document may be used as a reference to ensure the correct request is made.

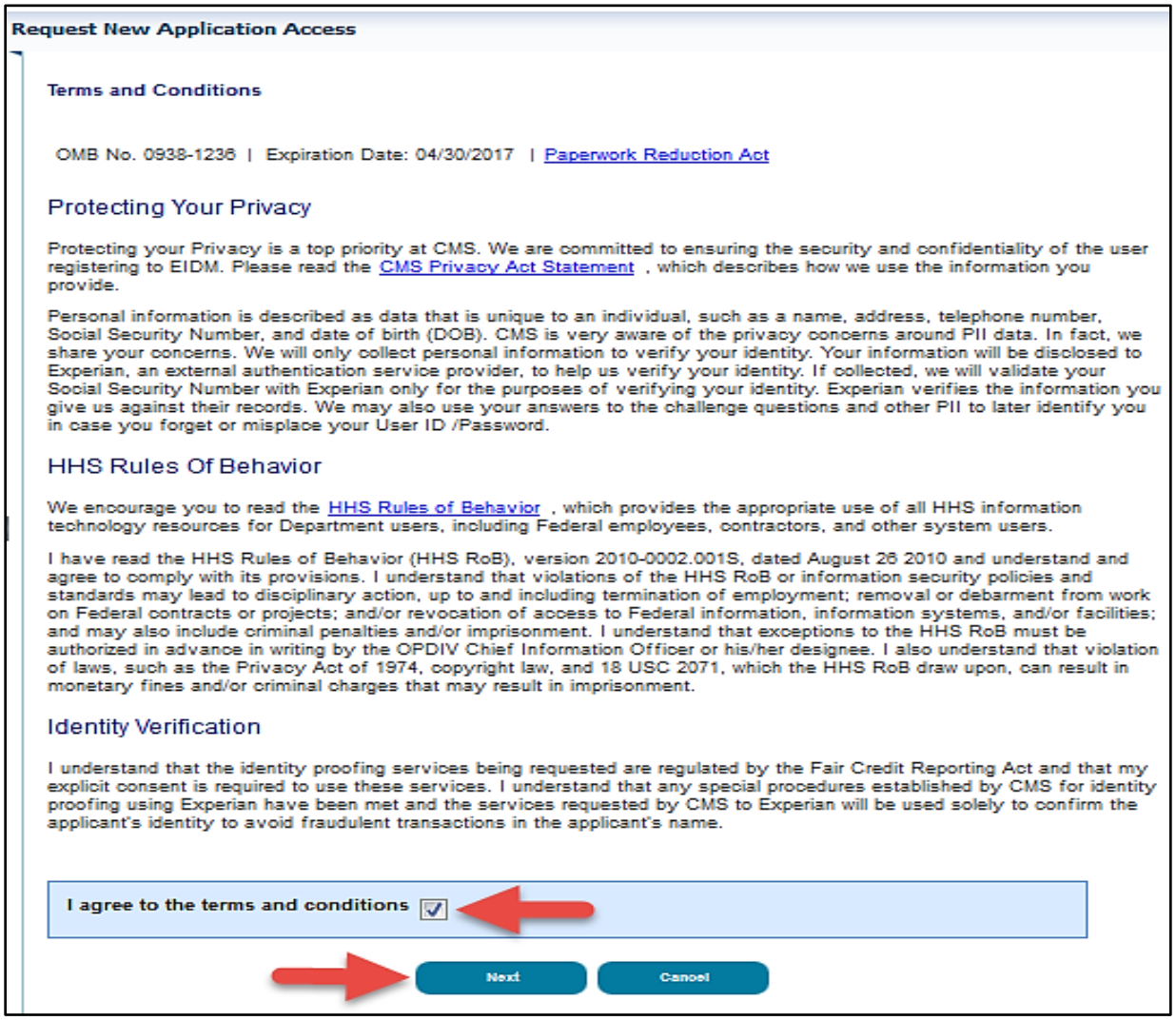


7. Select '**Next'** to complete the '**Identity Verification**' section. The Identity Verification process will only be completed the first time a user requests a role in the Physician Quality and Value Programs domain in EIDM.

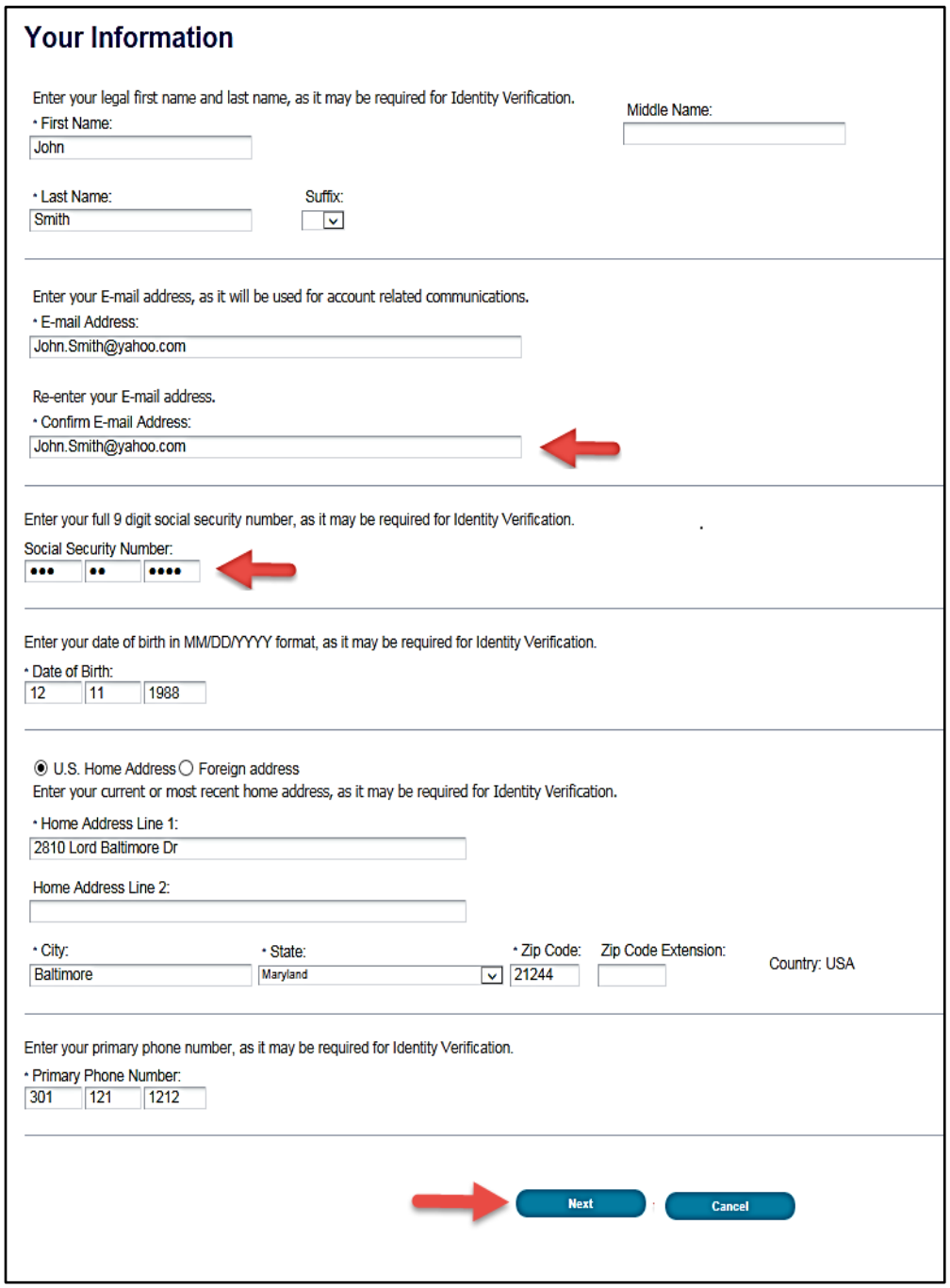
NOTE: If the Identity Verification has been completed, users can skip to step 16 to request additional roles.



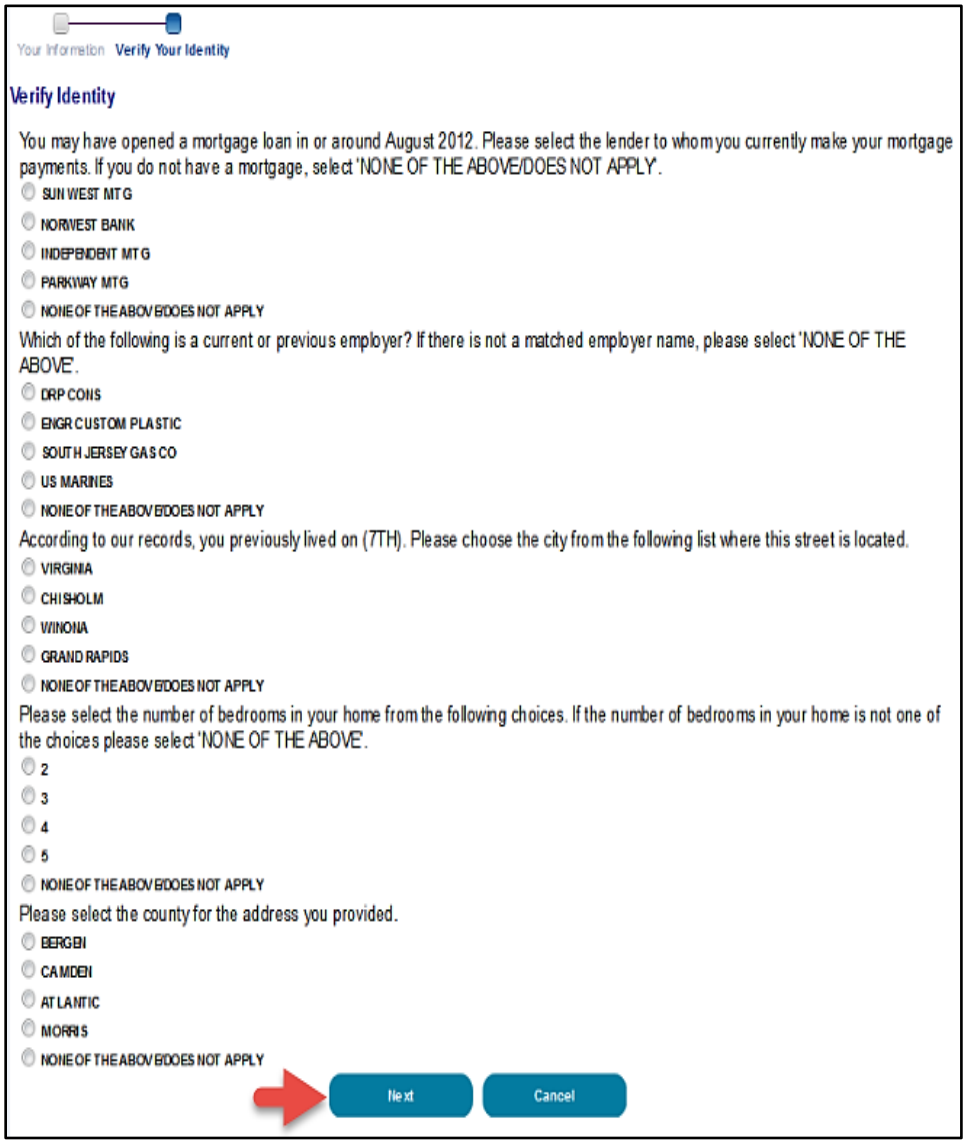
8. Read the Terms and Conditions. Select the '**I agree to the terms and conditions'** checkbox and then select '**Next'**, which will be enabled only after checking the **'I agree to the terms and conditions**' checkbox.



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

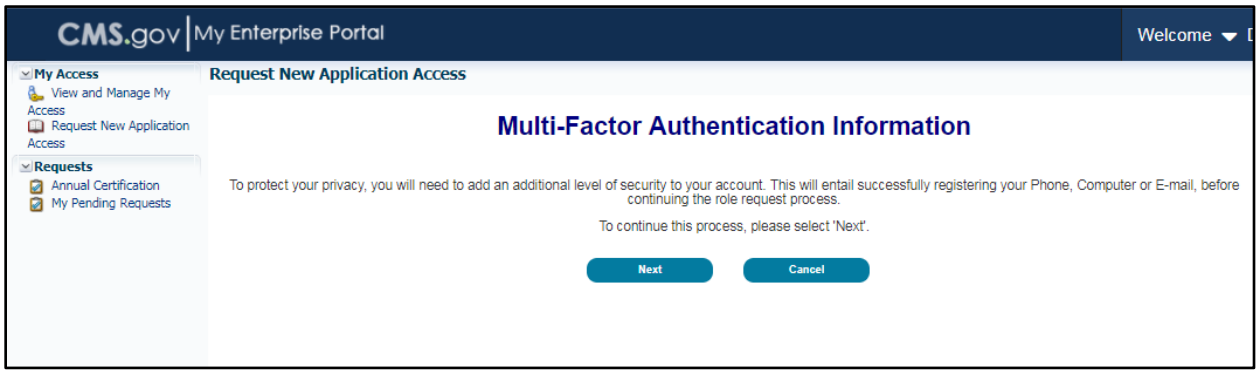


10. Select an answer to each question under ‘Verify Identity’. Select ‘Next’ after providing an answer to each question. ‘Verify Identity’ question information is provided from Experian in association with the SSN Number provided in step 10.

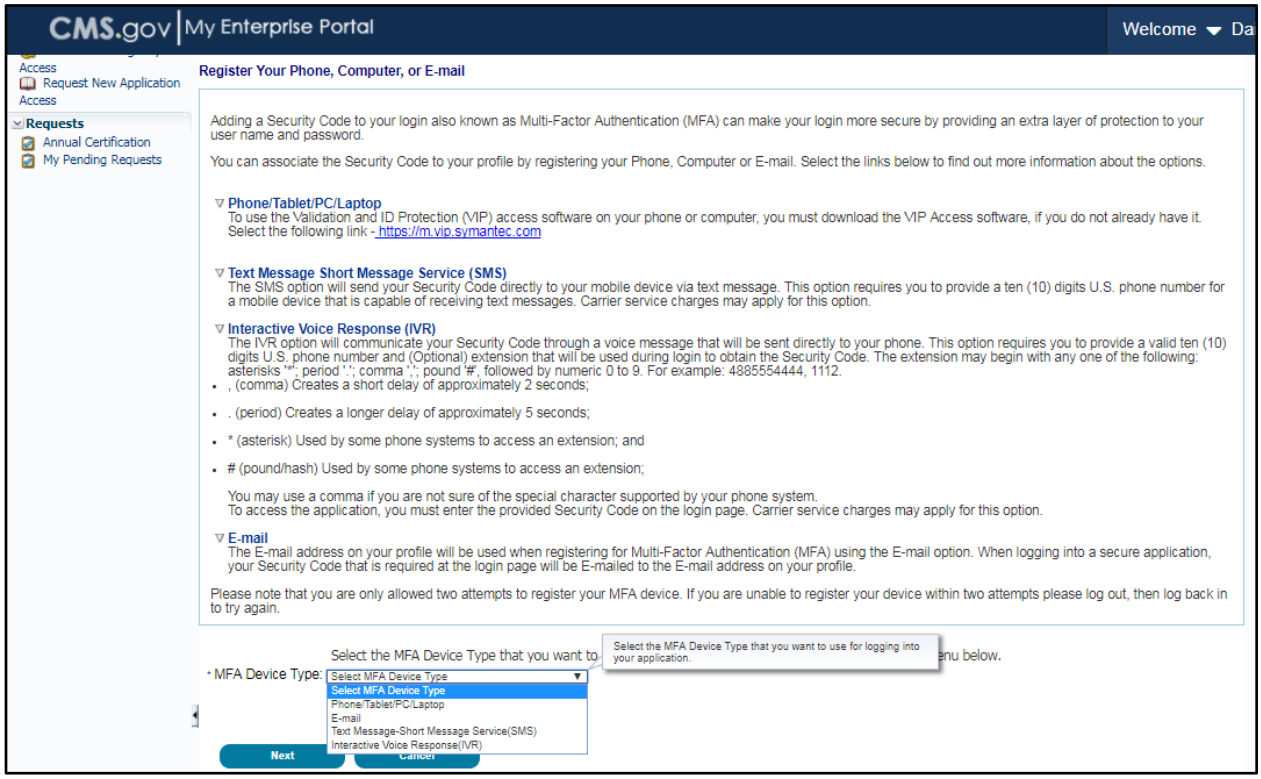


11. Remote Identity Proofing is now complete. Select '**Next'** to proceed to the '**Multi-Factor Authentication Registratio**n' process.

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 '**MFA Device Type'** drop-down menu.



14. 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 (https://vip.symantec.com/). If the VIP Access Software is not installed on your device, you will be unable to complete the Multi-Factor Authentication process.

    - Credential ID
    - MFA Device Description

    (b) If selecting E-mail One Time Password (OTP) as Credential Type, the E-mail address on your profile will automatically be used for the E-mail option to obtain the security code and the following required information fields will be displayed:

    - MFA Device Description

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

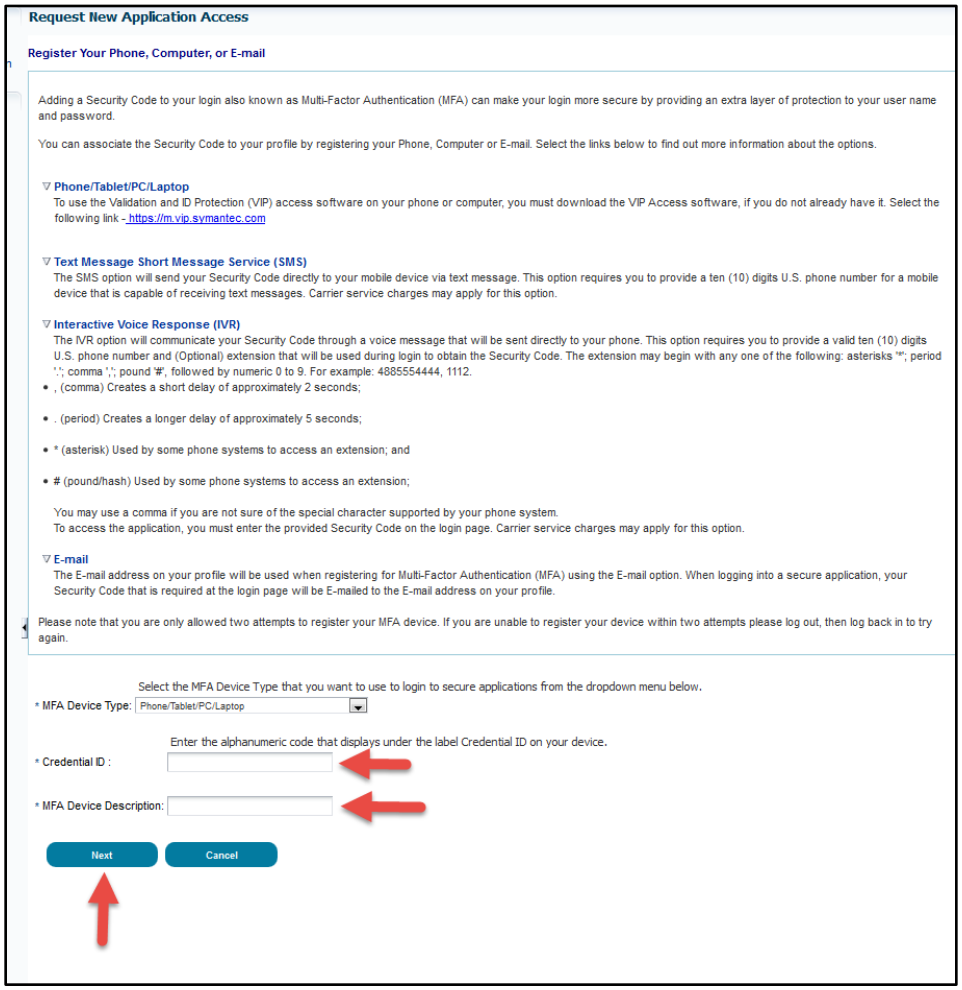
    - Phone Number

- MFA Device Description

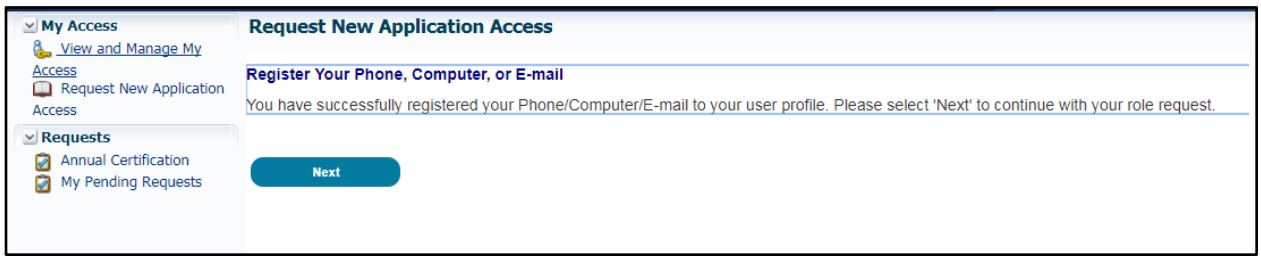
(d) If selecting Interactive Voice Response (IVR) as Credential Type, the following required information fields will be displayed:

- Phone Number and Extension
- MFA Device Description

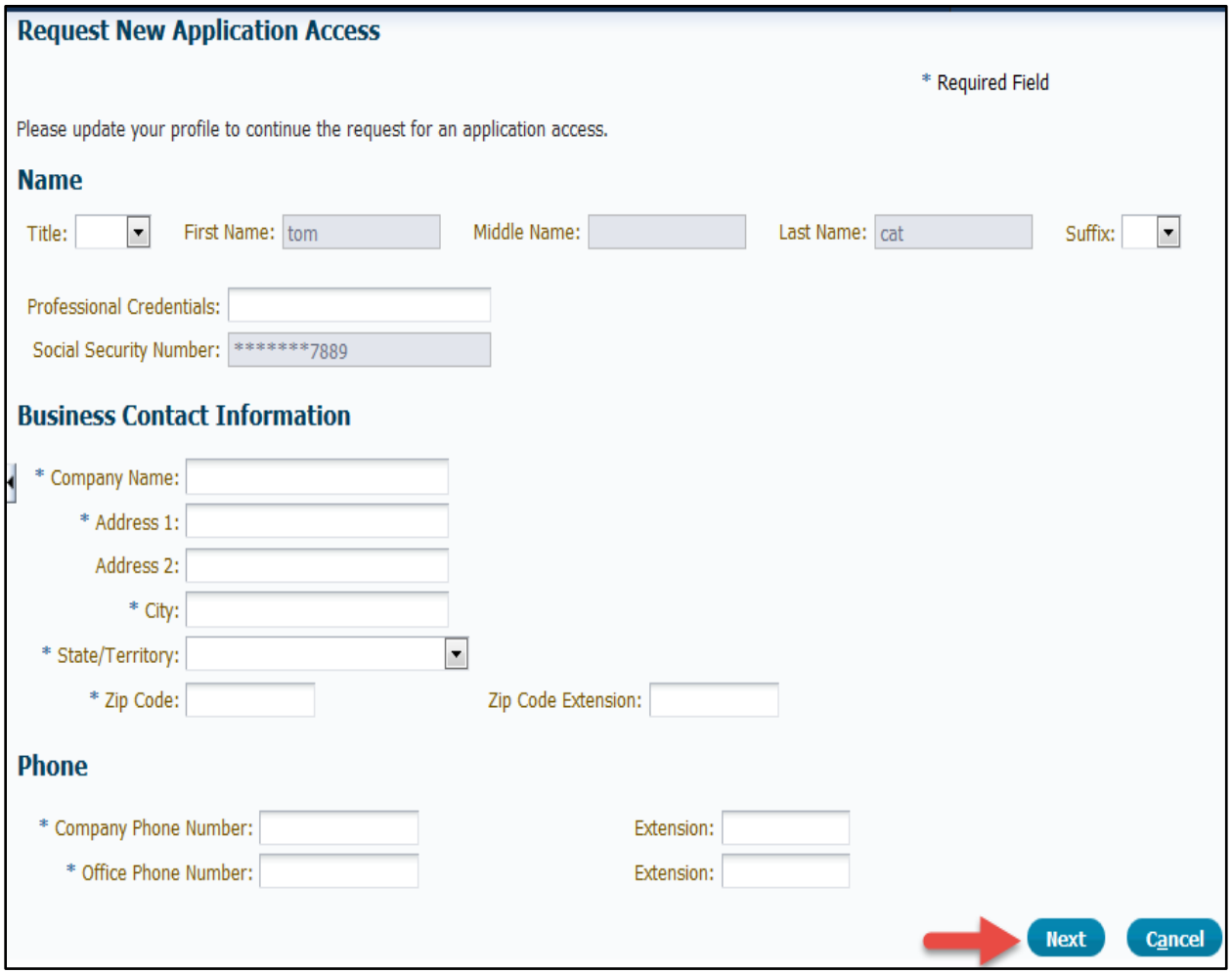
After providing the required information, select ‘Next’.



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



16. On the **Request New Application Access** page, provide the required information under the **Business Contact Information** and **Phone** sections. *Note that the information in the Name section will be pre-populated with the Remote Identity Proofing information.*



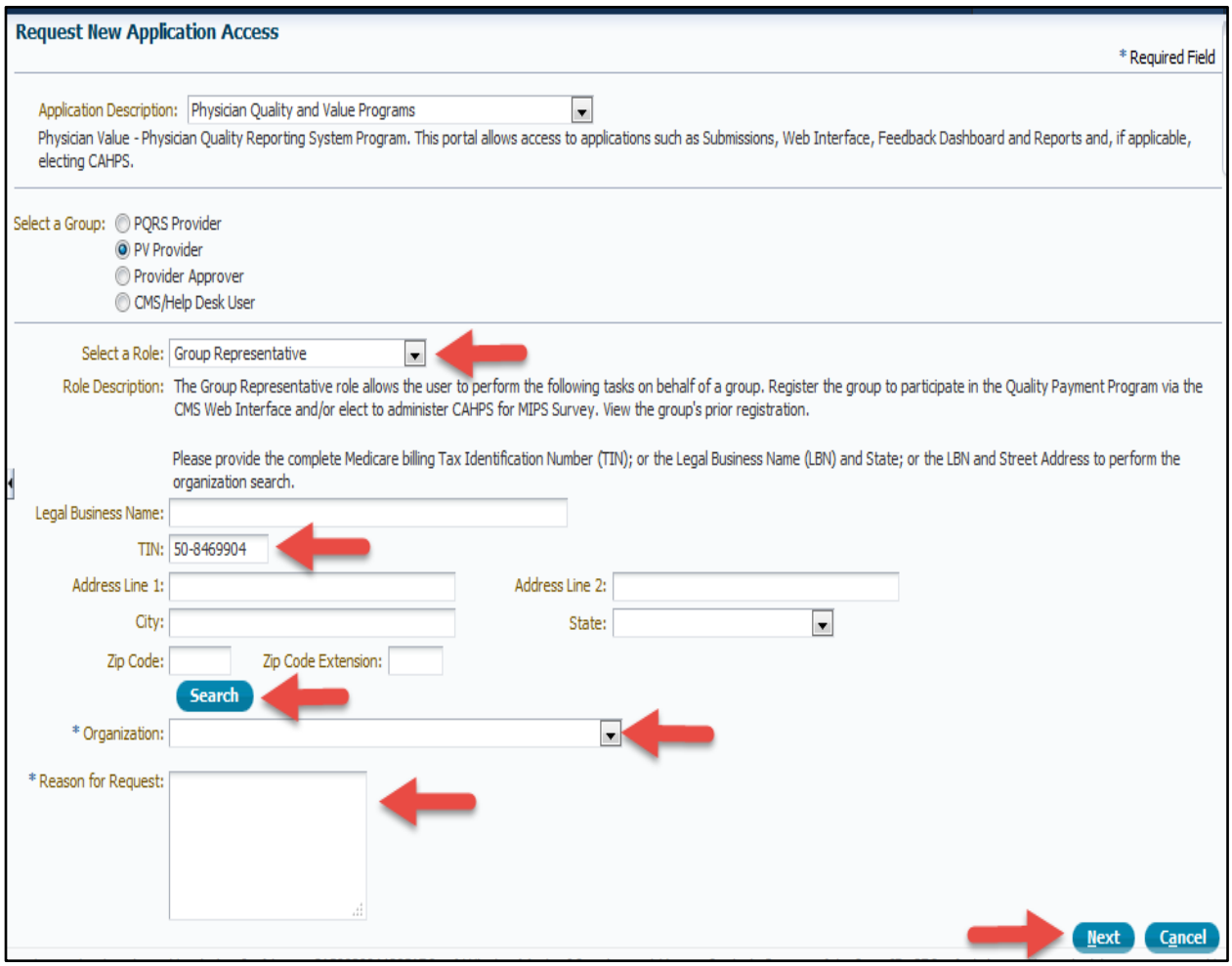
17. Search for the organization or individual practitioner:
    a. Enter one of the following for the organization or individual practitioner:
        - Medicare Billing TIN (preferred search criteria)

        OR

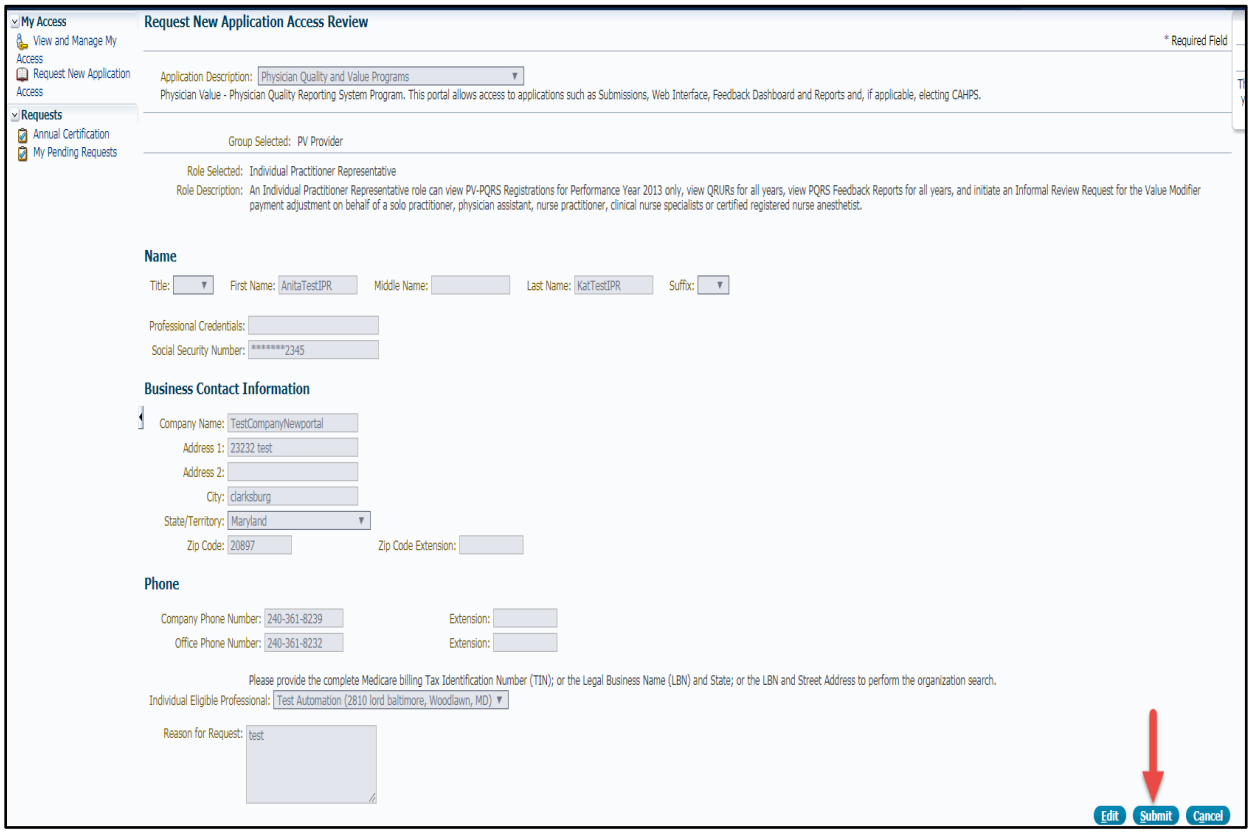
        - Legal Business Name and State

        OR

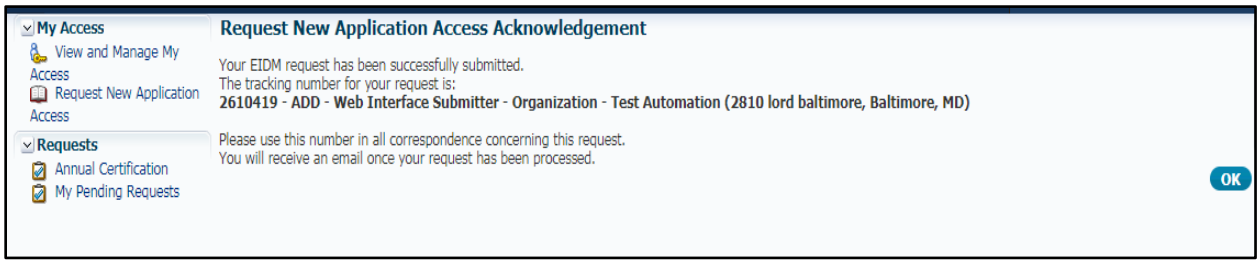
        - Legal Business Name and Street Address
    b. Select **Search**
    c. Select the group practice from the **Organization** drop-down menu.
    d. Enter a **'Reason for Request'** then select **'Next'**



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



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 above role requests will be directed to the appropriate approver(s) for the organization or Individual Practitioner 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.

If you have questions or need further assistance, please contact the Quality Payment Program using the contact information at the bottom of each page of this guide.