

Enterprise Identity Management (EIDM)

MODULE 3: ACO PROVIDER APPROVER ROLE

GPRO Web Interface Key Dates

- **Sampled beneficiaries available in the Web Interface for viewing and download:**
 - January 3-6, 2017
- **Training version of the Web Interface available:**
 - January 9-13, 2017
- **Enter and submit 2016 quality data through the Web Interface:**
 - January 17 – March 17, 2017 (closes at 8:00pm Eastern Time)

Introduction

- The EIDM training modules are based on material in the EIDM Quick Reference Guides (QRG), available for download at https://qnpapp.qualitynet.org/pqrs/eidm_guide.htm.
- The Shared Savings Program ACO EIDM Account and Role Set-up Guide is available on the Shared Savings Program ACO Portal under the Program Announcement, “2016 Quality Measurement and Reporting Guides.”
 - Available for download after logging into the CMS Enterprise Portal at <https://portal.cms.gov>.
- For Next Generation ACO Model, please reference <https://app.innovation.cms.gov/NGACOConnect> for additional guidance.

A Note on Screenshots

- Please note that screenshots in this presentation are taken from the QRGs and/ or a test EIDM system. They may not match exactly what you see in the live EIDM system.

GPRO Web Interface Roles in EIDM

- In order to submit data via the Web Interface, you must have **Web Interface Submitter** role for **your organization** (PQRS group practice or SSP/Pioneer/Next Generation ACO) in the EIDM.
- **Organization** must exist in EIDM prior to **Web Interface Submitter** role request.
- **Organization** is created by the user who requests **Provider Approver** role during this role's request process.
- **Organization** is created when the **Provider Approver** role for the Physician Quality and Value Programs application is approved.

Provider Approver Roles in EIDM

- There are two types of EIDM **Provider Approver** roles for those who are using the Web Interface:
 - ✓ **Security Official** applicable for PQRS Group Practices
 - ✓ **ACO Security Official** applicable for Accountable Care Organizations
- This module will discuss the **ACO Security Official** Provider Approver role. Please see Module 2 for a discussion of the **Security Official** Provider Approver role.

ACO Security Official Provider Approver Role

ACO Security Official role is applicable for ACO organizations identified by a primary and participant TINs.

ACO Security Official role assumes **Provider Approver** responsibility for the created ACO organization in EIDM, which includes:

- ✓ Approval of all **Provider** roles for this organization including other ACO Security Official roles
- ✓ Role management and recertification for the organization.

Current ACO Organization Limitation in EIDM

- ACO organization is identified by the following mandatory attributes:
 - ✓ ACO Primary TIN
 - ✓ ACO ID
 - ✓ ACO Program Name (Pioneer and MSSP only)
 - ✓ Two (2) Participant TINs
- Mandatory attributes should be provided in order to create an organization.

ACO Security Official Role Request

- To request a role in EIDM, you must first have an EIDM account.
- If you do not have a user ID and password, please see Module 1 on how to create an EIDM account.
- See next slides for requesting **ACO Security Official** role in EIDM.

Log into CMS Enterprise Portal

- Begin by navigating to <https://portal.cms.gov>.
 - The CMS Enterprise Portal home page is displayed.
 - Once on the page, select the **Login to CMS Secure Portal** link and enter your EIDM user ID and password.

The screenshot shows the CMS.gov Enterprise Portal. The header includes the CMS.gov logo, navigation links (Home, About CMS, Newsroom, Archive, Help & FAQs, Email, Print), and a search bar. Below the header, there are buttons for 'Health Care Quality Improvement System' and 'Provider Resources'. The main content area features a large banner with the text 'Welcome to CMS Enterprise Portal' and a description: 'The CMS Enterprise Portal is a gateway being offered to allow the public to access a number of systems related to Medicare Advantage, Prescription Drug, and other CMS programs.' To the right of the banner is a 'CMS Secure Portal' section with a 'Login to CMS Secure Portal' button and links for 'Forgot User ID?', 'Forgot Password?', and 'New User Registration'. At the bottom, there is a row of buttons for various CMS programs (CMS Enterprise Portal, MACBIS, Medicare Shared Savings Program, Physician Value, ASP, Open Payments, QMAT, CPC, Innovation Center, MLMS, MCU, PECOS, CBIC) and a section for 'CMS Provides Health Coverage for 100'.

CMS.gov | Enterprise Portal
Centers for Medicare & Medicaid Services

Home | About CMS | Newsroom | Archive | Help & FAQs | Email | Print

Learn about [your healthcare options](#) Search CMS.gov

Health Care Quality Improvement System Provider Resources

CMS Portal > Welcome to CMS Portal

Welcome to CMS Enterprise Portal

The CMS Enterprise Portal is a gateway being offered to allow the public to access a number of systems related to Medicare Advantage, Prescription Drug, and other CMS programs.

CMS Secure Portal

To log into the CMS Portal a CMS user account is required.

Login to CMS Secure Portal

[Forgot User ID?](#)
[Forgot Password?](#)
[New User Registration](#)

CMS Enterprise Portal | MACBIS | Medicare Shared Savings Program | Physician Value | ASP | Open Payments | QMAT | CPC | Innovation Center | MLMS | MCU | PECOS | CBIC

CMS Provides Health Coverage for 100

Information for people with Medicare, [Medicare open enrollment, and benefits.](#)

Get E-Mail Alerts Non-Production Environments

<https://portalval.cms.gov/wps/portal/unauthportal/home/#>

Terms and Conditions Screen

- This will take you to a screen showing the terms and conditions of using the EIDM.
 - You must agree to the terms and conditions in order to continue.
 - Read the **Terms and Conditions**, select **I Accept** to continue.

Terms and Conditions

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

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

By using this information system, you understand and consent to the following:

You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system.

At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.

Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.

To continue, you must accept the terms and conditions. If you decline, your login will automatically be cancelled.

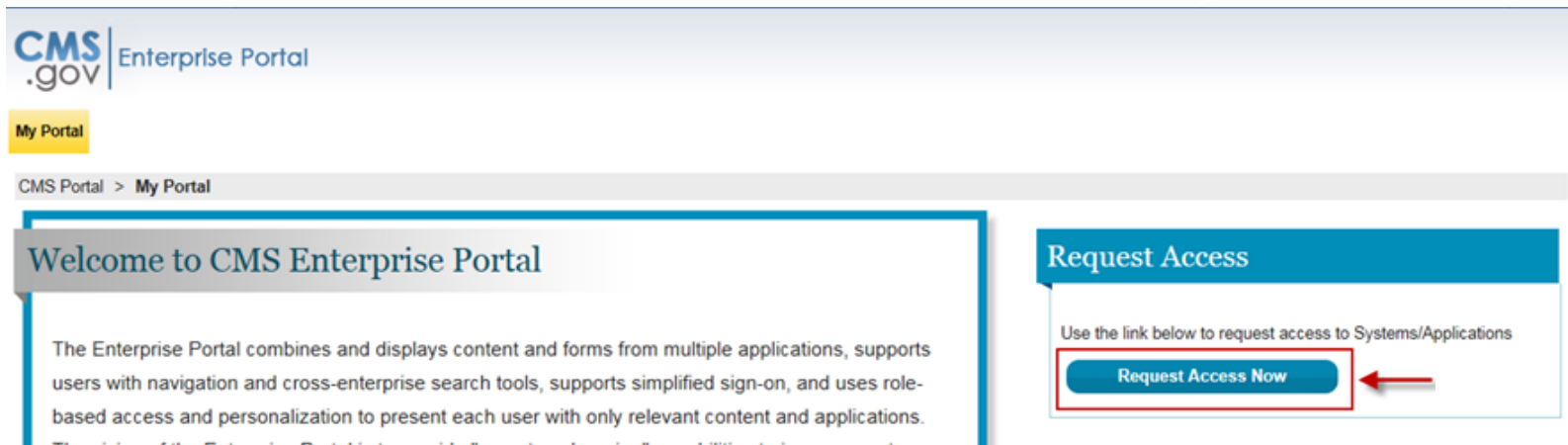


I Accept

Decline

Welcome to the CMS Portal

- The **Welcome to the CMS Enterprise Portal** page is displayed.
- Select the **Request Access Now** link.



Requesting Access

- Locate the **Physician Quality and Value Programs** domain on the left side of the screen and click on **Request Access** action button.
- Use two scroll bars located on the right side of the screen for navigating EIDM applications.

Novitasphere Internet Provider Portal for Novitas Solutions, Inc. Help Desk Information 855-880-8424 tmtesting@yahoo.com Request Access	OPENPAYEMENTS The Open Payments system satisfies the reporting requirement in Centers for Medicare & More... Help Desk Information 1-855-326-8366 Openpayments@cms.hhs.gov Request Access	Perf-PVPQRS Physician Value - Physician Quality Reporting System Program. This portal allows access to More... Help Desk Information 866-288-8912 tmtest@yahoo.com Request Access
Physician Quality and Value Programs Physician Value - Physician Quality Reporting System Program. This portal allows access to More...  Help Desk Information 866-288-8912 tmtest@yahoo.com Request Access	POLICYAPP POLICYAPP Help Desk Information TBD TBD Request Access	PS&R/STAR Provider Statistical and Reimbursement/System for Tracking Audit and Reimbursement. More... Help Desk Information 866-484-8049 tmtesting@yahoo.com Request Access
PV-PQRS RIDP/MFA Physician Value - Physician Quality Reporting System Program. This portal allows access to More... Help Desk Information 866-288-8912 tm.testing@yahoo.com Request Access	QMAT The Quality Measures Assessment Tool (QMAT) application allows users to submit clinical da More... Help Desk Information TBD TBD Request Access	SHIM SHIM is the Small Business Health Options Program Marketplace that helps businesses provid More... Help Desk Information TBD TBD Request Access

Provider Approver Role

- 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**.

My Access

- Modify Business Contact Information
- View and Manage My Access
- Request New Application Access

Requests

- My Pending Requests

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

Cancel

Select ACO Security Official

- The **ACO Security Official** role will be selected for those users that are a part of a Medicare Shared Savings Program or Pioneer ACO organization.
- For Next Generation ACO Model, please see additional guidance at <https://app.innovation.cms.gov/NGACOConnect>.

Portal Help & FAQs | Print | Log Out | Welcome EIDM User

CMS.gov Enterprise Portal

My Portal

CMS Portal > EIDM user menu page > My Access

My Access

- View and Manage My Access
- Request New Application Access

Requests

- My Pending Requests

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:

- Approver Roles
- ACO Security Official**
- Security Official
- Individual Practitioner

Cancel

iHelp
Select a Role
Select a value from the options being displayed.

https://eidmi.cms.gov/iacs/faces/pages/authenticated/main.jspx?action=addAccess&appId=37

Identity Verification

- You will then be taken to the identity verification section.
- Select **Next** to complete the **Identity Verification** section.

The screenshot shows a web interface for 'My Portal'. At the top, a yellow button labeled 'My Portal' is visible. Below it, a breadcrumb trail reads 'CMS Portal > EIDM user menu page > My Access'. A status bar indicates 'Screen reader mode Off | Accessibility Settings'. The main content area is titled 'My Access' and contains two links: 'Request New System Access' and 'View and Manage My Access'. The 'Identity Verification' section is highlighted, containing a paragraph about privacy and a list of three bullet points. At the bottom of this section are two buttons: 'Cancel' and 'Next'.

My Portal

CMS Portal > EIDM user menu page > My Access

Screen reader mode Off | Accessibility Settings

My Access

[Request New System Access](#)

[View and Manage My 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.

- 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.
- 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.
- 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'.

Cancel Next

Identity Verification (cont'd)

- 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 this step.

Terms and Conditions

- This will take you to a screen showing the terms and conditions of using the EIDM.
- You must agree to the terms and conditions in order to continue.
 - Click the box next to the statement **I agree to the terms and conditions.**
 - Then, click on the **Next** button.

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

Consent To Monitoring

By logging onto this website, you consent to be monitored. Unauthorized attempts to upload information and/or change information on this web site are strictly prohibited and are subject to prosecution under the Computer Fraud and Abuse Act of 1986 and Title 18 U.S.C. Sec.1001 and 1030. We encourage you to read the [HHS Rules of Behavior](#) for more details.

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.

Collection Of Personal Identifiable Information (PII)

"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 data to uniquely identify the user registering with the system. 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.

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.

☒ I agree to the terms and conditions

[Cancel](#) [Next](#)

Your Information

- You will then be taken to the **Your Information** page.
- You will need to complete the information request on this page. Please note that fields with an asterisk (*) are required fields and have to be completed.
- After all required information has been provided, select **Next** to continue.

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:

Entering Your Information

- 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.

Identity Verification

- 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 Social Security Number provided.

[Request New System Access](#)

[View and Manage My Access](#)

Verify Identity

You may have opened an auto loan in or around July 2014. Please select the lender for this account. If you do not have such an auto loan, select 'NONE OF THE ABOVE/DOES NOT APPLY'.

- ☐ FIRST UNION
- ☐ WELLS FARGO BANK
- ☐ BANK ONE
- ☐ FORD MOTOR CREDIT CO
- ☐ NONE OF THE ABOVE/DOES NOT APPLY

You may have opened a student loan in or around May 2012. Please select the lender that you have previously or you are currently making payments to. If you have not received student loans with any of these lenders now or in the past, please select 'NONE OF THE ABOVE/DOES NOT APPLY'.

- ☐ US BANK
- ☐ PANHANDLE PLNS STUDNT
- ☐ SALLIE MAE
- ☐ COMMERCE BANK
- ☐ NONE OF THE ABOVE/DOES NOT APPLY

Please select the term of your auto loan (in months) from the following choices. If your auto loan or auto lease term is not one of the choices please select 'NONE OF THE ABOVE'.

- ☐ 24
- ☐ 36
- ☐ 48
- ☐ 60
- ☐ NONE OF THE ABOVE/DOES NOT APPLY

You may have opened a mortgage loan in or around March 2014. 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'.

- ☐ FREDDIE MAC
- ☐ SUN WEST MTG
- ☐ COLONIAL MORTGAGE
- ☐ LOAN AMERICA
- ☐ NONE OF THE ABOVE/DOES NOT APPLY

Multi-Factor Authentication

- Remote **Identity Verification** is now complete.
 - Select **Next** to proceed to the **Multi-Factor Authentication Registration** process.
- You are now at the screen to begin the multi-factor authentication step.
 - Select **Next** to begin registration for **Multi-Factor Authentication Information** process.



Multi-Factor Authentication (cont'd)

- You will need to register either a phone, computer or email address.
- Read through the descriptions of each of these options on this screen and then select an option from the **MFA Device Type** drop-down menu.

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 adding a second factor to your user name and password.

You can associate the Security Code to your profile by registering your phone, computer or E-mail. Select one of the following options.

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

Please note that you are only allowed two attempts to register your MFA device. If you are unable to register, you will be locked out for 15 minutes. You can then return back in to try again.

Select the MFA Device Type that you want to register into your application.

* MFA Device Type:

E-mail Address:

* MFA Device Description:

The E-mail address on your profile will automatically be used for the E-mail option. You can also register a different E-mail address for MFA registration. To change your E-mail, please select 'Change E-Mail Address' from the 'My Profile' page.

Multi-Factor Authentication (cont'd)

- If selecting **Phone/Tablet/PC/Laptop** as **MFA Device Type**, the following required information fields will be displayed:
 - Credential ID
 - MFA Device Description
 - NOTE: If you intend to use your mobile device or computer then you must download the VIP software.
- If selecting **E-mail** as **MFA Device Type**, the following required information fields will be displayed:
 - E-mail
 - MFA Device Description
- If selecting **Text Message – Short Message Service (SMS)** as **MFA Device Type**, the following required information fields will be displayed:
 - Phone Number
 - MFA Device Description
- If selecting **Interactive Voice Response (IVR)** as **MFA Device Type**, the following required information fields will be displayed:
 - Phone Number
 - MFA Device Description
- After providing the required information, select **Next**.

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 adding a second factor 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 MFA Device Type that you want to register.

➤ **Phone/Tablet/PC/Laptop**

➤ **Text Message Short Message Service (SMS)**

➤ **Interactive Voice Response (IVR)**

➤ **E-mail**

Please note that you are only allowed two attempts to register your MFA device. If you are unable to register, please wait 15 minutes and try again.

Select the MFA Device Type that you want to register:

• MFA Device Type:

E-mail Address:

The E-mail address on your profile will automatically be used for the E-mail option. To change your E-mail, please select 'Change E-Mail Address' from the 'My Profile' page.

• MFA Device Description:

Selecting the Approver Role

- Registration for the **Multi-Factor Authentication** is now complete, but you still need to request the appropriate role.
 - Select **Next** to proceed to request the role.
- Recall that **Security Official** is for PQRS Group Practices and **ACO Security Official** is for Pioneer, Next Generation, and Medicare Shared Savings ACOs.
 - In this module, we are going to select the **ACO Security Official** role.

Organization Information

- You will need to select either **Create an Organization** or **Associate to an Existing Organization**

Creating an Organization

- The first user registering on behalf of the organization will select **Create an Organization**.
- Complete the required information, including entering a **Reason for Request**, then select **Next**.

The screenshot shows a web application interface for creating a new organization. The left sidebar contains a 'My Access' menu with options like 'Modify Business Contact Information', 'View and Manage My Access', and 'Request New Application Access'. Below it is a 'Requests' section with 'My Pending Requests'. The main content area is titled 'Request New Application Access' and 'Create New Organization'. It includes an 'Application Description' dropdown set to 'Physician Quality and Value Programs'. Under 'Select a Group', 'Provider Approver' is selected. 'Select a Role' is set to 'Security Official'. The 'Create/Associate' section has 'Create an Organization' selected. A red box highlights the main form fields, with red arrows pointing to the 'Create an Organization' radio button, the 'PTAN 1' field, and the 'Next' button at the bottom right. The form fields include: TIN, Group Unique Identifier, ACO Parent TIN, Legal Business Name, NPI 1, PTAN 1, NPI 2, PTAN 2, NPI 3, PTAN 3, Address Line 1, City, Zip Code, Country (United States), Phone Number, Extension, Fax Number, Email, Website, Address Line 2, State, Zip Code Extension, and Reason for Request.

Creating an Organization (cont'd)

- Please make sure that the Primary TIN (ACO TIN) and the CMS ACO ID are used for the ACO organization.
- When creating a new organization if you are a part of a Medicare Shared Savings Program or Pioneer ACO organization, you have 3 attempts to enter 2 valid participant TINs, with an automated approval process.
 - If you fail the 3 attempts, then your information will be submitted to the QualityNet Helpdesk for review.

Creating an Organization (cont'd)

- When creating a new organization if you are a part of a Next Generation ACO organization or a single TIN ACO, you have 3 attempts to enter the valid participant TINs before being routed to the **QualityNet HelpDesk Approver** for manual approval.
 - For single TIN ACOs, this is due to the minimal available TIN information for data entry, which requires a manual review.
 - If further assistance is needed, contact the QualityNet Helpdesk.

Associating to an Existing Organization

- Other users registering with an existing EIDM organization will select **Associate to an Existing Organization**.
- Enter the search criteria and select the appropriate organization.

The screenshot shows a web application interface for requesting new application access. The left sidebar contains a 'My Access' menu with options like 'Modify Business Contact Information', 'View and Manage My Access', and 'Request New Application Access'. Below it is a 'Requests' section with 'My Pending Requests'. The main content area is titled 'Request New Application Access' and 'Associate to Existing Organization'. It includes a dropdown for 'Application Description' set to 'Physician Quality and Value Programs'. Below this is a 'Select a Group' section with radio buttons for 'PQRS Provider', 'PV Provider', 'Provider Approver' (selected), and 'CMS/Help Desk User'. A 'Select a Role' dropdown is set to 'Security Official'. The 'Role Description' text explains the role. The 'Create/Associate' section has two radio buttons: 'Associate to an Existing Organization' (selected and highlighted with a red box and arrow) and 'Create an Organization'. Below this is a text prompt: '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.' A red box encloses the search fields: 'Legal Business Name', 'TIN', 'Address Line 1', 'City', 'Zip Code', 'Zip Code Extension', and 'Address Line 2'. A red arrow points to the 'Search' button. At the bottom, there is a 'Reason for Request' text area and 'Next' and 'Cancel' buttons. A red arrow points to the 'Next' button.

My Access

- Modify Business Contact Information
- View and Manage My Access
- Request New Application Access

Requests

- My Pending Requests

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

Application Description: Physician Quality and Value Programs
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: Security Official
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:
City:
Zip Code: Zip Code Extension:

Address Line 2:
* Reason for Request:

Associating to an Existing Organization (cont'd)

- 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.
- When associating to an existing organization, the request will be sent to the **ACO Security Official** for approval.

Application Acknowledgement

- A tracking number will be displayed on screen, and is also sent via email to the requestor.
 - This tracking number should be retained until the requested role has been applied to the account.
- Click **OK**.



Application Approval

- The approver, who is the Security Official or ACO Security Official, will only receive an email notifying them of disapproval, as the approval process is automated.
- The notification of approval, denial, or other requests will be sent to the role requestor's email address on file for the request.

Help with EIDM

QualityNet Helpdesk

Monday – Friday:
7:00 AM – 7:00 PM (Central Time)

E-mail: qnetsupport@hcqis.org

Phone: 866-288-8912

TTY: 877-715-6222

Fax: 888-329-7377