Quality Payment PROGRAM

Connect to an Organization and Select a Role

Table of Contents

Introduction

This document outlines the steps to Connect to an Organization (like a practice or QCDR/Registry) and how to get the Security Official or Staff User role you need.

The role you select for each organization will allow you to:

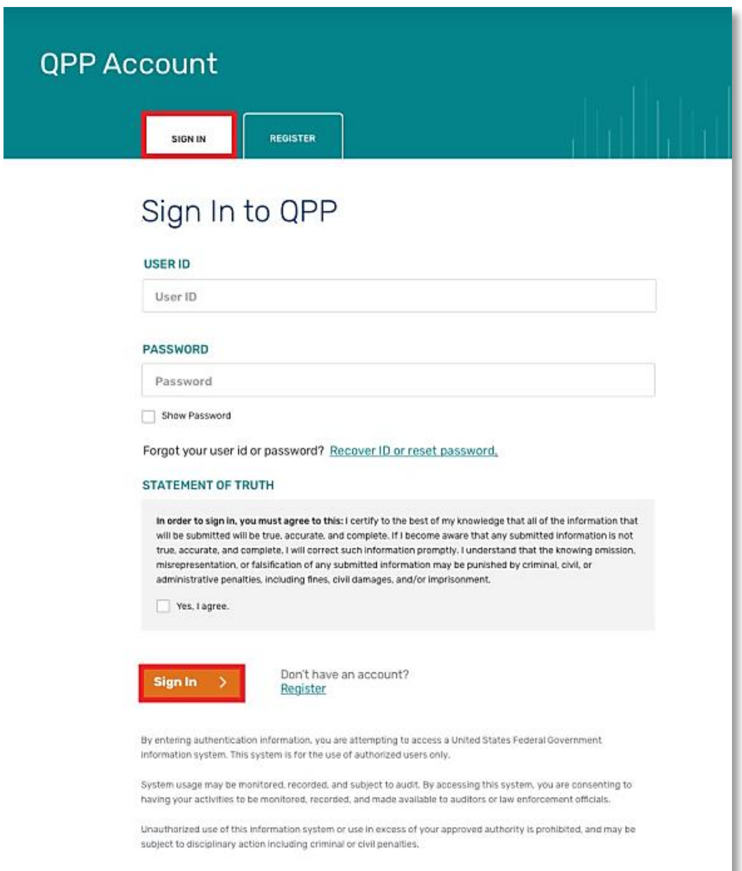
- View information (like performance feedback), or
- Perform an action (like submitting performance data).

If you are a new user or an existing user requesting access to an organization, you'll need to understand which organization type to select and know which role you need.

Getting Started

Sign In to the Quality Payment Program

1. Go to the [Quality Payment Program Website]() and click **Sign In** on the upper right-hand corner.
2. Enter your **User ID** and **Password**.
3. Check **Yes, I agree** next to the Statement of Truth and click **Sign In**.
   - You will be prompted to provide a **security code** from your two-factor authentication.



Returning users:
Sign in with the same credentials you've previously used.

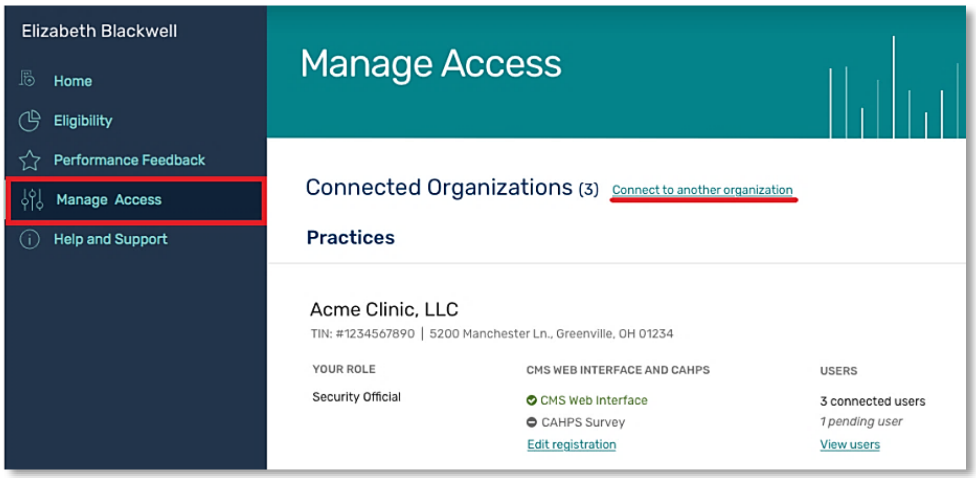
New users:
Sign in with your newly created HARP credentials.

Don't have an account?
Click Register next to Sign In and review the **Register for a HARP Account document** in this guide.

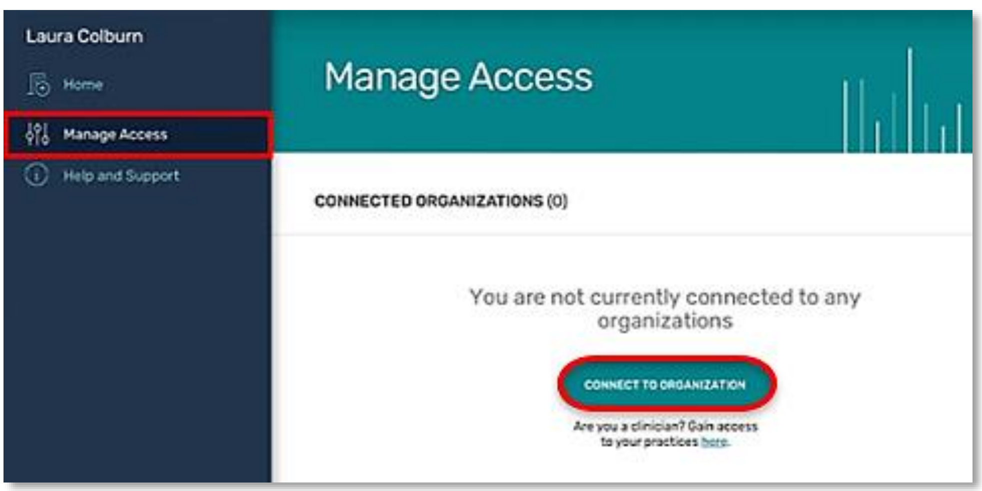
Navigate to Manage Access

Click **Manage Access** on the left-hand navigation pane. If you are a:

- **Returning user:** You will see a **list of organizations** that you're currently connected to.
  - **Review** and **confirm** that the list of connected organizations and roles are correct. If correct, no further action is required.
  - If you need to connect to another organization, you can by clicking the **connect to another organization** link.



- **New Users:** Will be prompted to **connect to an organization**.



Connect to an Organization Step-by-Step Instructions

Overview

Now that you have successfully signed into qpp.cms.gov and navigated to **Manage Access**, follow these steps to **Connect to an Organization**:

1. Choose your organization type
2. Find your organization
3. Select your role

Then you can review your confirmed role requests (pending or automatic approved)

Reminder:

There's a special role available to clinician's. Check out the **Connect as a Clinician document** in this guide for more information.

We will begin with **selecting an organization type**. This step is the **same for all organization types**.

Important Notes:

- Each organization **must** have a **Security Official** before anyone can request a Staff User role or additional Security Official roles.
- Contact an administrator in your organization to let them know your organization needs a Security Official if that's not an appropriate role for you.
- If you need access to **multiple organizations**, you will need to complete the above steps for **each** organization you want to connect with.

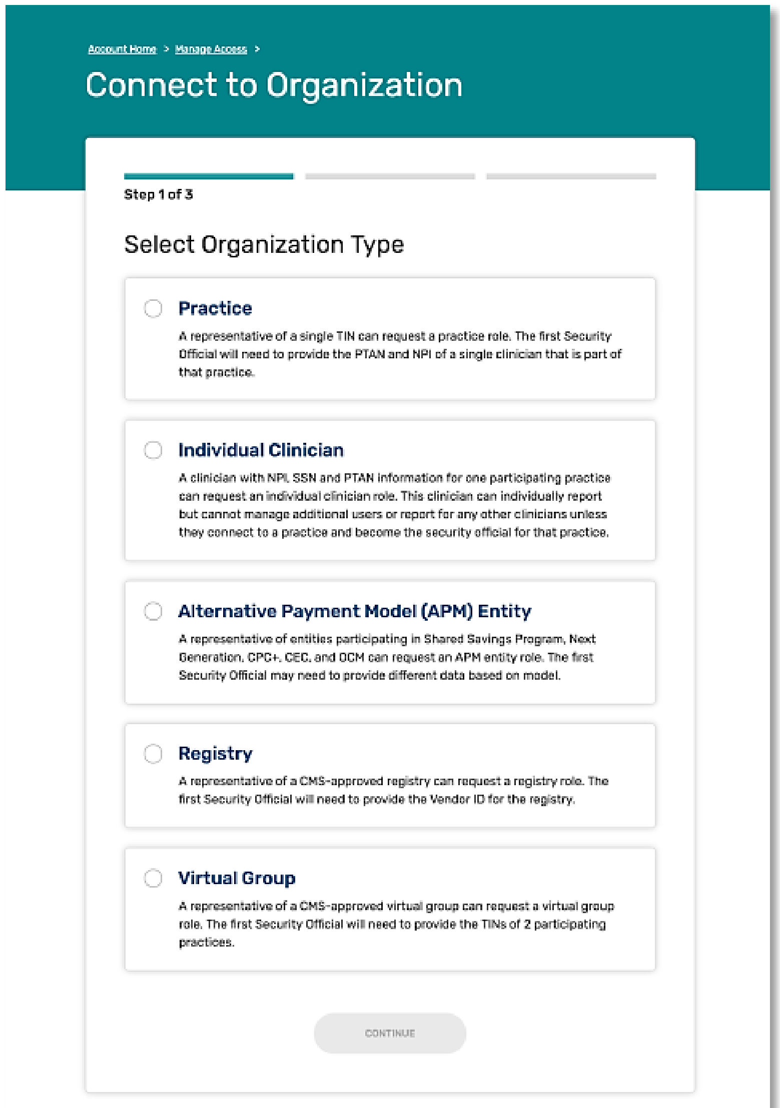
Step 1: Select Organization Type

Select which **organization type** you'd like to connect to. After you select an organization type, click **continue.**

The organization types are:

- Practice
- *Individual Clinician (refer to the Connect as a Clinician document* in this guide*)*
- Alternative Payment Model (APM) Entity
- Registry (Includes Qualified Registries and Qualified Clinical Data Registries)
- Virtual Group

Note: If you are connecting to multiple organizations, you will need to complete a request for **each** organization one at a time.



Looking for more information on Organization Types?
Continue onto the **next page** for more information on selecting an organization type.

Which Organization Type Do I Select?

There are four organization types you can choose from:

Organization Type	Description	Helpful Hint
Practice	Connect to a **Practice** if you represent an organization identified by a single Taxpayer Identification Number (TIN), like a solo/individual practitioner, group, or hospital including: • Groups or clinicians that need to report performance data. • Groups that participate in a Shared Savings Program ACO (all tracks) or clinicians scored under the APM scoring standard that need to submit group-level date for the Promoting Interoperability performance category. • Electronic Health Record (EHR) or other Health Information Technology (HIT) Vendors will need to complete this request for each practice they represent/are submitting data for on [qpp.cms.gov](qpp.cms.gov).	Solo CPC+ practitioners (those who are the only clinician in their Practice Site) will need to connect to an **APM Entity** to submit their electronic clinical quality measures (eCQMs) for the CPC+ program and view your complete performance feedback. Individual clinicians can also request the **Clinician role**, for more information check out the **Connect as a Clinician document**.
Individual Clinician	*Check out the Connect as a Clinician document in this Guide for additional information on connecting as a clinician.*	

Organization Type	Description	Helpful Hint
APM Entity	Connect to an **APM Entity** if you represent a Shared Savings Program ACO entity, Next Generation ACO entity, CPC+ Practice Site, ESCO, or OCM Practice Site and need to submit Quality data on behalf of the entire entity or want to view the Entity's performance feedback. **Note**: If you are connecting to multiple organizations, you will need to complete a request for each organization one at a time.	You will connect to an APM Entity if you need to perform an action, like submitting Quality data, on behalf of the entire Entity or view the Entity's MIPS performance feedback. Unless representing the entire Entity, clinicians, groups and solo practitioners who participate in an APM will typically need to connect to a **Practice** to report other data required under the APM scoring standard.
Registry *(Including Qualified Registries and QCDRs)*	Connect to a **Registry** if you represent a CMS-approved **Qualified Registry** or a **Clinical Data Registry (QCDR)** and are submitting data on behalf of your clients. **Note**: If you represent a previously approved Registry or QCDR, you will need the Security Official role to complete the self-nomination application on qpp.cms.gov.	You will connect to a Registry when you are a representative of a Qualified Registry or QCDR. Clinicians, groups and virtual groups working with a Registry or QCDR for data collection and submission would connect to a **Practice** (or **virtual group** as appropriate) to view performance feedback and data submitted on their behalf by those vendors. Individual clinicians can also request the **Clinician role**, for more information check out the **Connect as a Clinician document** in this guide.

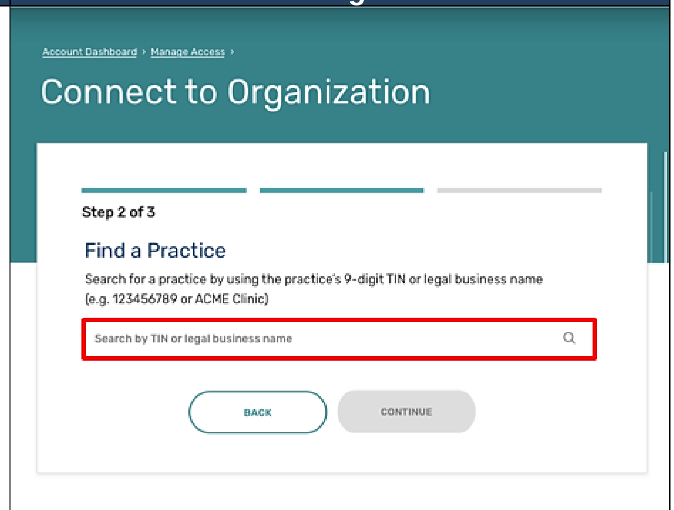
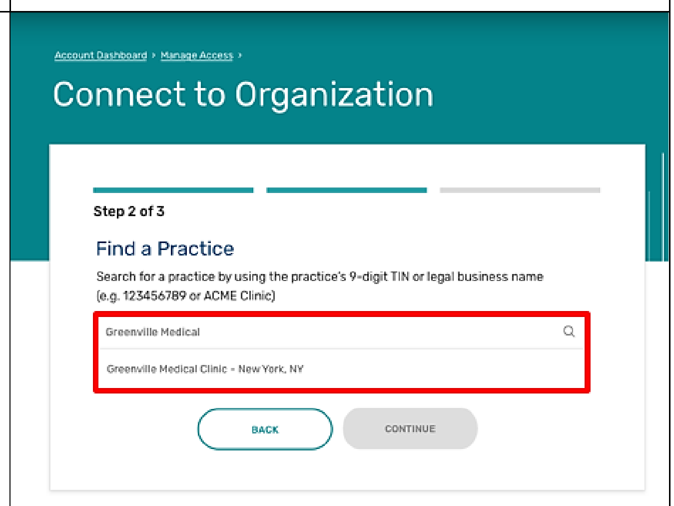
Step 2: Find Your Organization Type

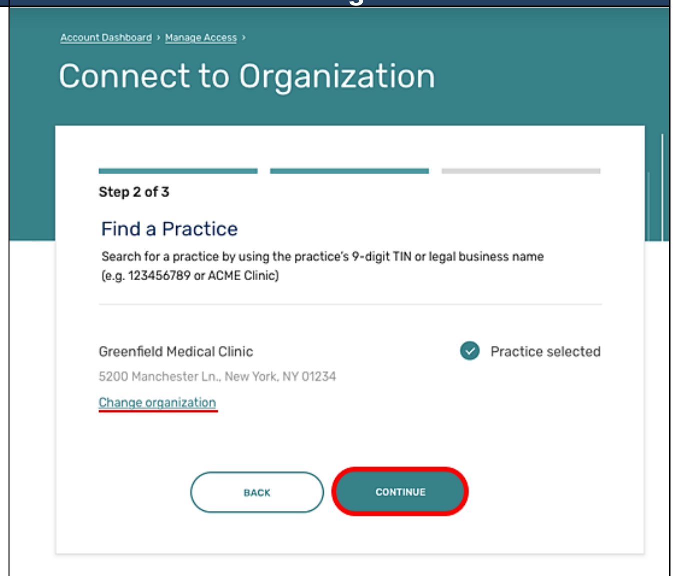
After you select your organization type, you will **find your organization** using search criteria. The search criteria is dependent upon your organization type.

Review the table below to determine what search criteria you can use to find your organization. Then, **click your organization type** for step-by-step instructions and images on how to find your organization type.

Organization type	Criteria you can use to search
Practice	• Legal Business Name; **OR** • Complete Taxpayer Identification Number (TIN) **without dashes** ✓ No search results will populate until you enter the complete TIN (9 digits)
APM Entity	**Step 1:** Identify your model (Shared Savings Program ACO, Next Generation ACO, Comprehensive Primary Care Plus (CPC+), Comprehensive ESRD Care (CEC) or Oncology Care Model (OCM)) **Step 2:** Provide: • Legal Business Name (APM Entity Name) • APM Practice Site ID (applicable to some models like CPC+ and OCM)
Registry *(Including Qualified Registries and QCDRs)*	• Legal Business Name; **OR** • Complete Taxpayer Identification Number (TIN) ✓ No search results will populate until you enter the complete TIN (9 digits, **without dashes**)
Virtual Group	• Complete Virtual Group ID

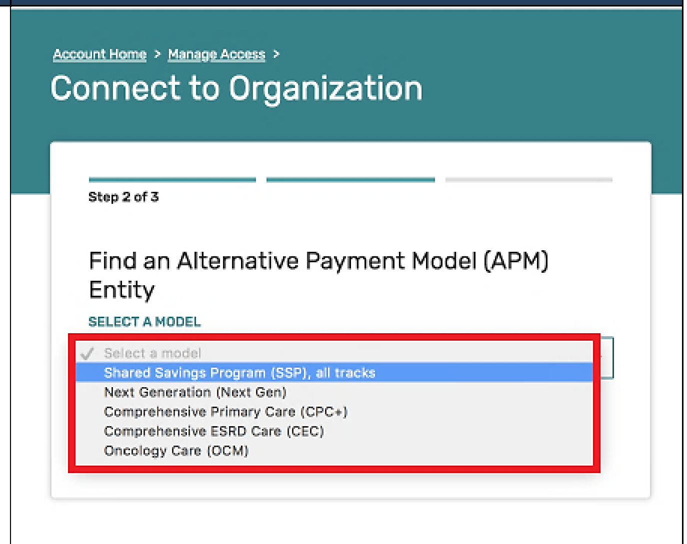
Practice

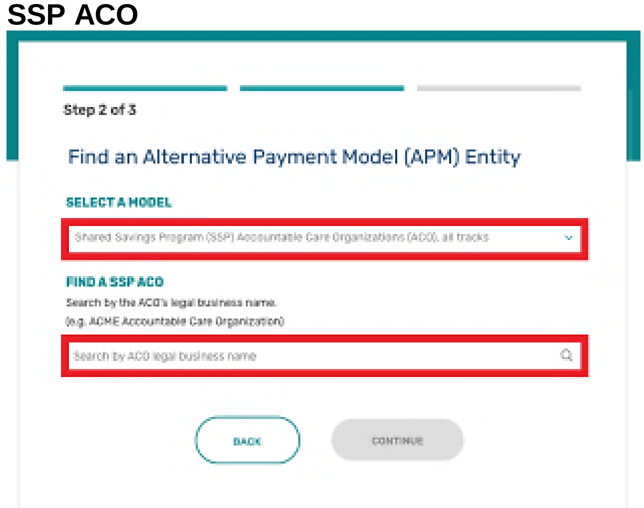
Action	Description	Image
Search for Practice	Search for the practice by TIN or legal business name. If you are searching by: • **Legal business name**: you can start typing and select the practice from the suggested potential matches based on what you've entered so far. • **TIN**: you will need to enter the complete TIN (**without dashes**) before a match is identified.	
Select Practice	Select the practice from the drop down and click **continue**.	

Action	Description	Image
Review Selection or Change Selected Practice	Review and confirm you selected the correct organization by clicking **continue**. **OR** Click the **Change Organization** link to update your practice selection if you selected the incorrect option.	

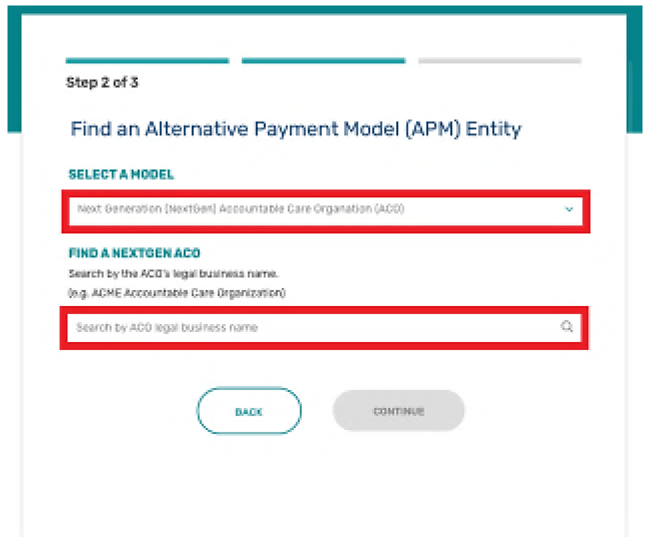
Ready to Select a Role?
Click here for Step 3: Select a Role

APM Entity

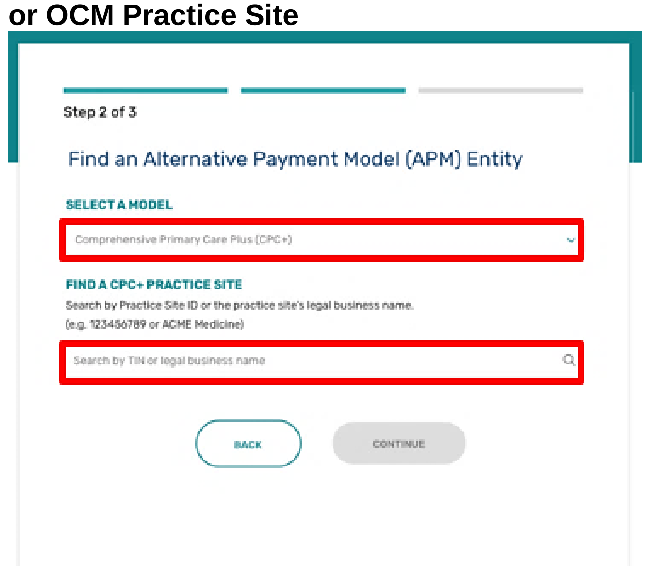
Action	Description	Image
Select a Model	Select the APM model you need to connect to from the drop-down menu: ✓ Shared Savings Program (SSPs) *all tracks* ✓ Next Generation (Next Gen) ✓ Comprehensive Primary Care (CPC+) ✓ Comprehensive ESRD Care (CEC) Model *all tracks* ✓ Oncology Care Model (OCM) *all tracks* Once the APM model is selected, click **continue**.	

Search for APM Entity	Search for the APM Entity, input fields will vary based on APM Model selected.
	Search by the following for each APM Model:
	• SSP ACO
	    ○ Legal business name
	• Next Generation ACO
	    ○ Legal business name
	• CPC+ Practice Site
	    ○ Practice Site legal business name
	    ○ CPC+ Practice ID
	• ESCO Organization Site (CEC)
	    ○ ESCO legal business name
	    ○ ESCO ID
	• OCM Practice Site
		SSP ACO
		

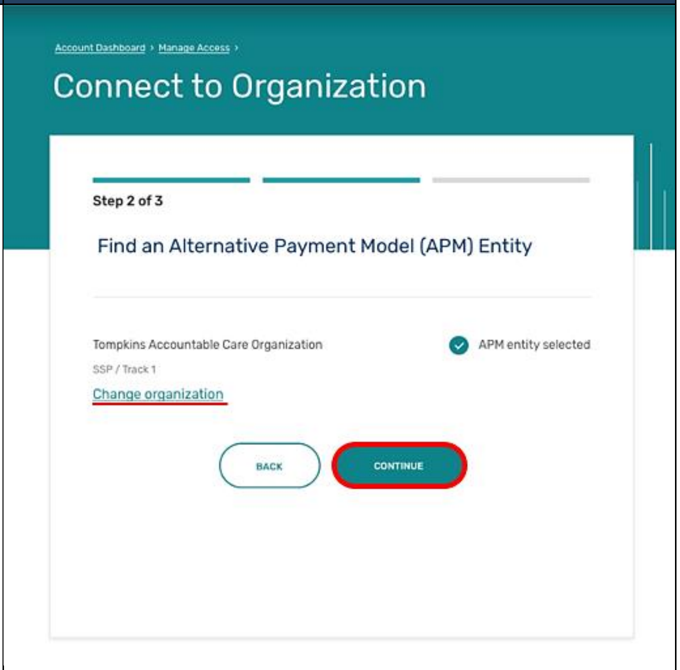
<table>
<tr><th>Action</th><th>Description</th><th>Image</th></tr>
<tr><td></td><td>
Practice Site legal business name
OCM ID
</td><td>
Next Generation



CPC+ Practice Site, ESCO Organization Site, or OCM Practice Site

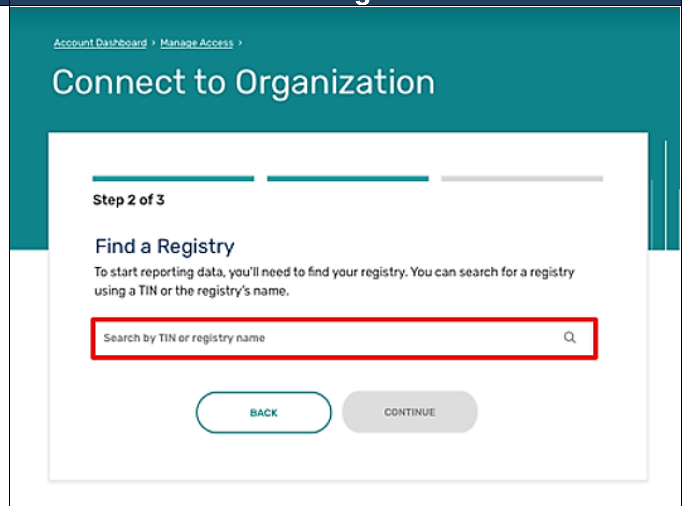
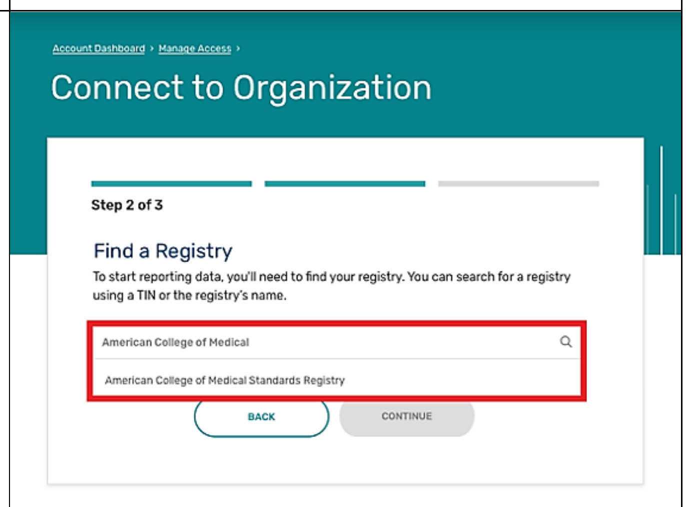


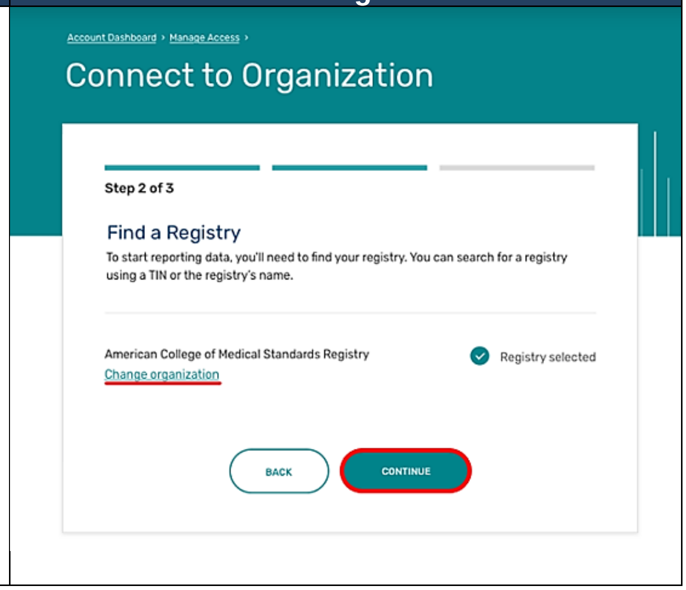
</td></tr>
</table>

Action	Description	Image
Review Selection or Change Selected APM Entity	Review and confirm you selected the correct organization by clicking **continue**. **OR** Click the **Change Organization** link to update your APM Entity selection if you selected the incorrect option.	

Ready to Select a Role?
Click here for Step 3: Select a Role

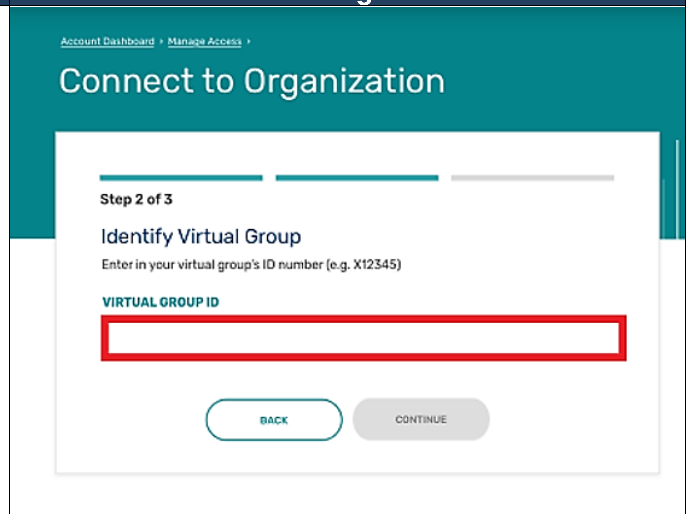
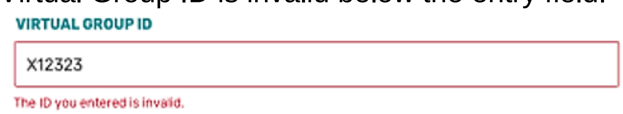
Registry

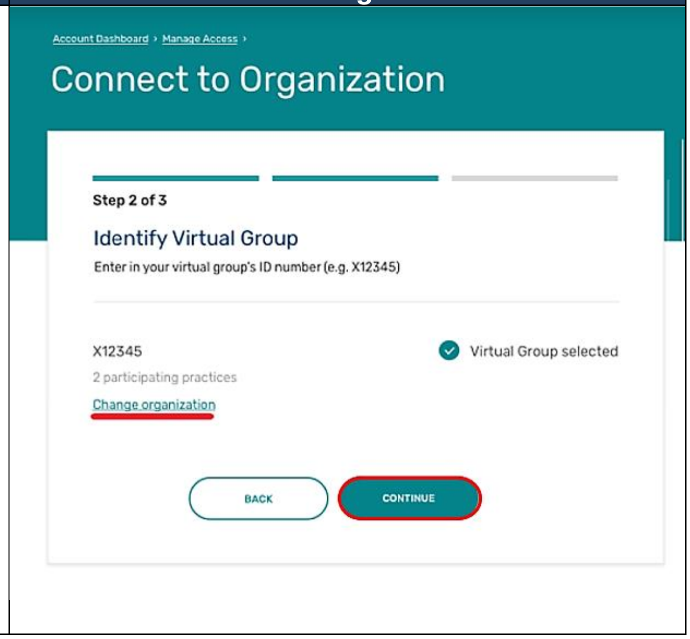
Action	Description	Image
Search for Registry	Search for the registry (including Qualified Registries and QCDRs) via TIN or Registry name. If you are searching by: • **Legal business name**: you can start typing and select the practice from the suggested potential matches based on what you've entered so far. • **TIN**: you will need to enter the complete TIN (**without dashes**) before a match is identified.	
Select Registry	Select the Registry from the drop down and click **continue**.	

Action	Description	Image
Review Selection or Change Selected Registry	Review and confirm you selected the correct organization by clicking **continue**. **OR** Click the **Change Organization** link to update your registry selection if you selected the incorrect option.	

Ready to Select a Role?
Click here for Step 3: Select a Role

Virtual Group

Action	Description	Image
Search for a Virtual Group	Search for the Virtual Group by entering your complete **Virtual Group ID**, then select **continue**.	 **Note**: If you enter an incorrect Virtual Group ID, you will receive a message noting that your Virtual Group ID is invalid below the entry field.  Please confirm you entered the correct Virtual Group ID if you encounter this message.

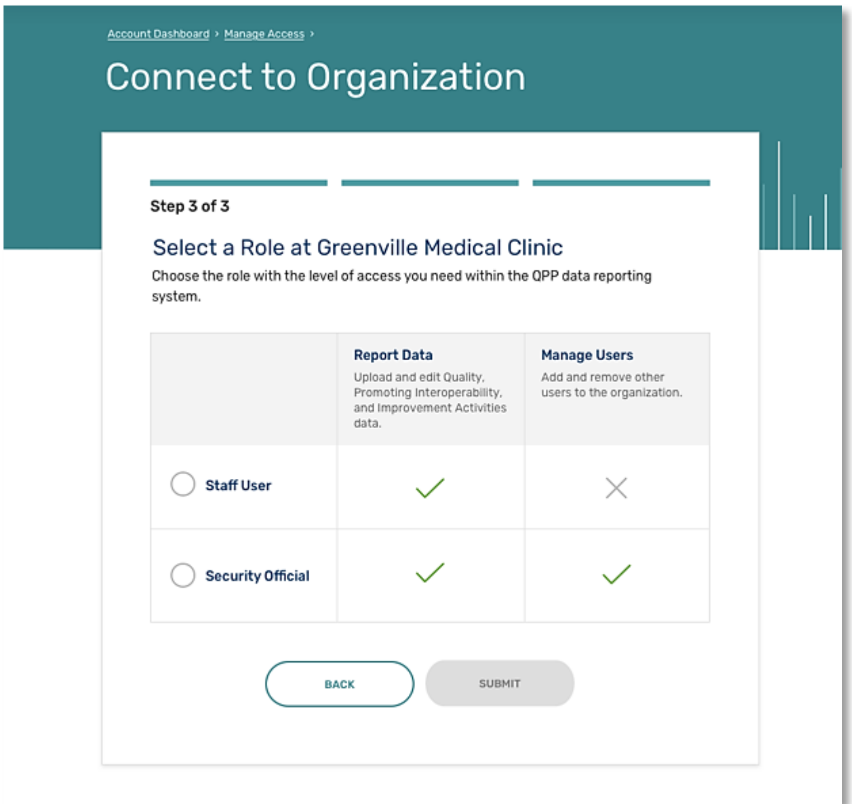
Action	Description	Image
Review Selection or Change Selected Virtual Group	Confirm that the **correct** virtual group was selected and select **continue**. **OR** Click the **Change Organization** link to update your virtual group selection if you selected the incorrect option.	

Ready to Select a Role?
Click here for Step 3: Select a Role.

Step 3: Select a Role

For **all organization types**, you have two roles to select from:

- The Staff User role
- The Security Official role (first Security Official or additional Security Official(s))
  - Each organization type must have a **first** Security Official before anyone can request a Staff User role or additional Security official roles.
  - The **first** Security Official will provide **additional information** during the validation process. The additional information requested will vary depending on organization type.



Looking for more information on these roles?

More information on the two QPP roles and what each role **lets you do**, is available on the

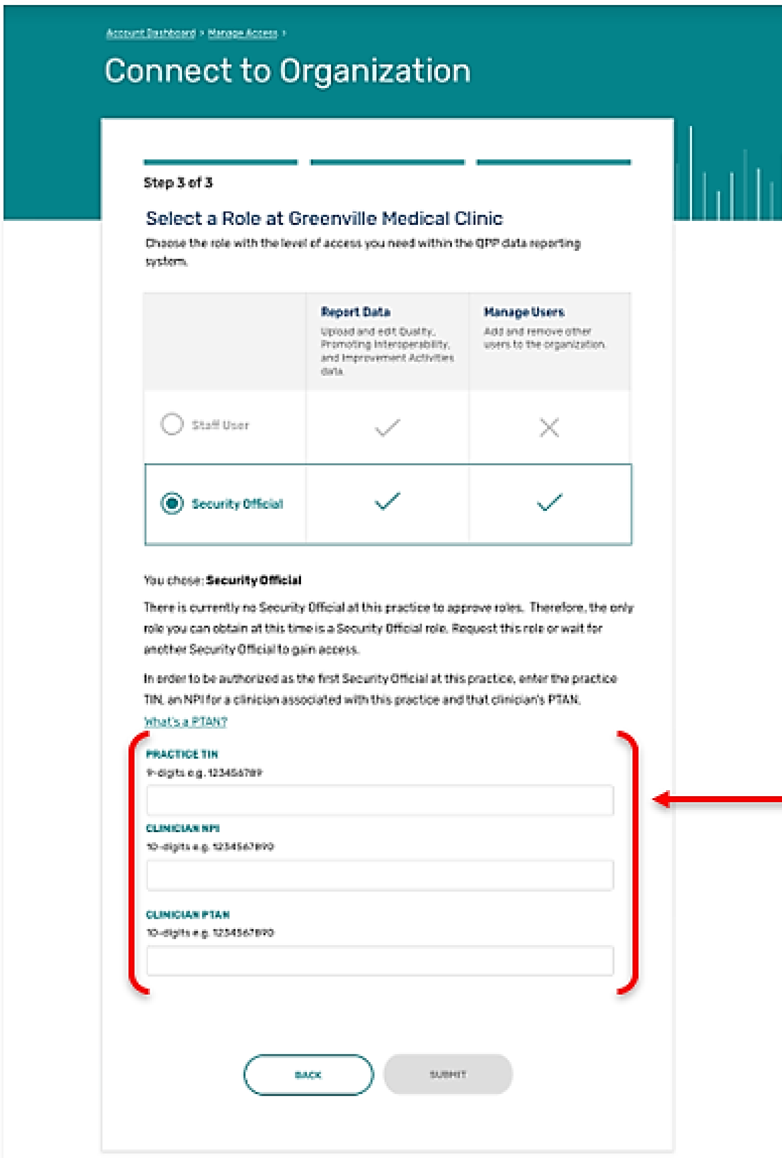
Which Role Should I Select?

Organization Type	Staff User Role Lets You	Security Official Role Lets You
Practice	✓ View eligibility information for all clinicians in the practice ✓ View claims measure data submitted during the performance period submitted ✓ View individual and group MIPS performance feedback and payment adjustment information ✓ Access the Physician Compare Preview ✓ Access APM incentive payments made to a TIN on behalf of an NPI Submit data on behalf of the practice, whether reporting **individually** or as a **group** ✓ Request a Targeted Review	Do everything the Staff User can do PLUS: ✓ Register a group for the **CMS Web Interface** ✓ Register a group for the **CAHPS for MIPS survey** ✓ **Approve all additional user requests** (manage access to the organization)
APM Entity	✓ Submit quality data on behalf of the Shared Savings Program ACO Entity, Next Generation ACO Entity, or CPC+ Practice Site ✓ View a list of participating practices and clinicians in the APM ✓ View eligibility information for participating practices and clinicians in the APM ✓ View MIPS performance feedback for the following models: o Shared Savings Program ACO o Next Generation ACO o Comprehensive Primary Care Plus (CPC+) o Comprehensive ESRD Care (CEC o Oncology Care Model (OCM)	Do everything the Staff User can do PLUS: ✓ **Approve all additional user requests** (manage access to the organization)

Organization Type	Staff User Role Lets You	Security Official Role Lets You
Registry *(Including Qualified Registries and QCDRs)*	✓ Submit data on behalf of all your clients ✓ View preliminary performance feedback for your clients based on the data you submitted on their behalf	Do everything the Staff User can do PLUS: ✓ **Approve all additional user requests** (manage access to the organization) ✓ Complete the **self-nomination application** on qpp.cms.gov (previously approved vendors only)
Virtual Group	✓ View a list of all the practices and clinicians participating in your virtual group ✓ Submit data on behalf of the virtual group ✓ View virtual group MIPS performance feedback	Do everything the Staff User can do PLUS: ✓ **Approve all additional user requests** (manage access to the organization) ✓ Register a group for the **CMS Web Interface** ✓ Register a group for the **CAHPS for MIPS survey**

First Security Official

If you are the **first** Security Official, select **Security Official**, and you will be prompted to enter [additional information] for **validation**. Once you enter the requested information, click **Submit.**



Next, if your validation is successful, you will be [**automatically** approved].

Remember: Each organization must have a **Security Official** before anyone can request a Staff User role or additional Security Official roles.
If Security Official is **not** the appropriate role for you, contact an administrator in your organization to let them know your organization needs a Security Official.

This section will vary by **organization type**. Continue onto the **next page** for more information on what **additional information** is required to validate the **first** Security Officials request.

Click here if you encountered an **error message**.

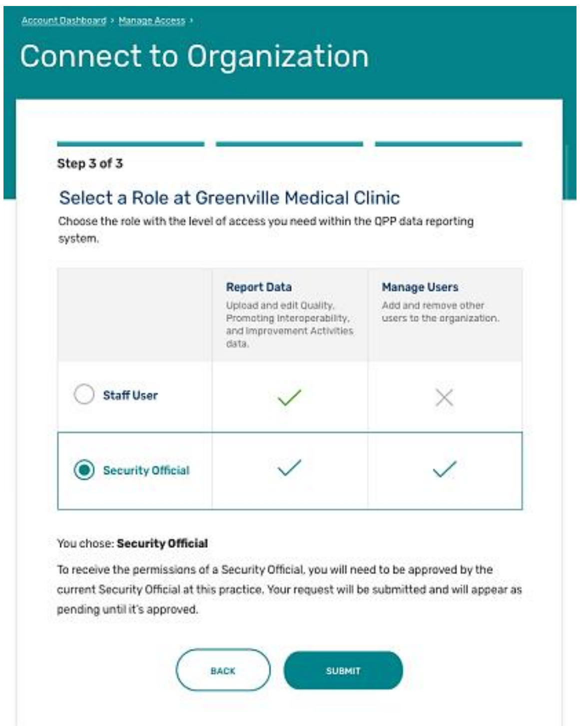
Additional Information Required for Validation of the Security Official Role

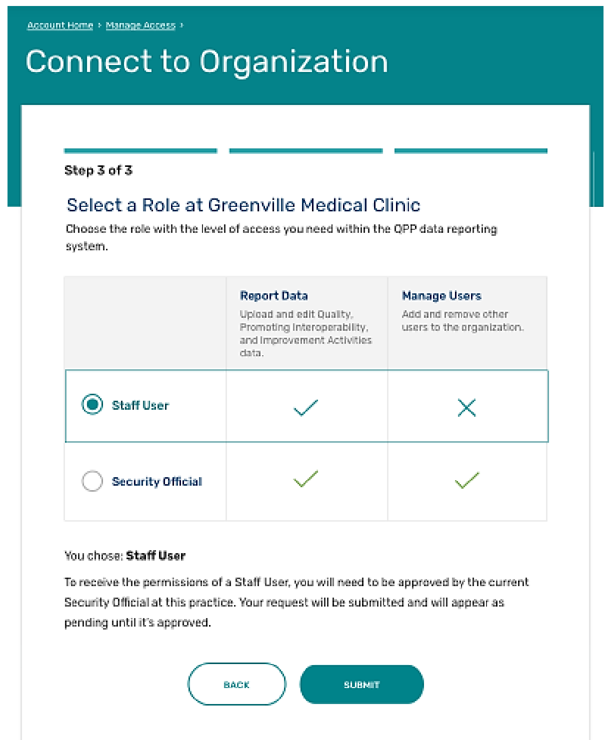
If you apply for the Security Official role, you'll need to provide some additional information to validate your credentials, the additional information is dependent upon your organization type.

Organization Type	Required Information	Additional Context
Practice	✓ The practice's Taxpayer Identification Number (TIN) ✓ The National Provider Identifier (NPI) of one clinician in the practice ✓ That clinician's Provider Transaction Access Number (PTAN)	Follow these steps to find PTANs in PECOS: 1. Log into Internet-based PECOS. 2. Select **My Associates** on PECOS home page. 3. Select **View Enrollments** by applicable individual or organizational enrollment. 4. Click on **View Medicare ID Report** 5. PTAN(s) are listed in Medicare ID column.
APM Entity – Shared Savings Program or Next Generation	✓ APM Entity ID (your ACO ID) ✓ The Taxpayer Identification Number (TIN) of two practices participating in the ACO	Security Officials for a single TIN ACO only need to provide one TIN
APM Entity – CPC+	✓ APM Entity ID (your Practice Site ID) ✓ The Taxpayer Identification Number (TIN) of a practice associated with the Practice Site ✓ The National Provider Identifier (NPI) of a clinician in the practice associated with the Practice Site	If your Practice Site includes multiple TINs, you can enter any of these TINs and an NPI associated with the Practice Site in that TIN
APM Entity - CEC	✓ APM Entity ID (your ESRD Seamless Care Organization ID) ✓ The Taxpayer Identification Number (TIN) of a practice associated with the Organization Site	If your ESCO includes multiple TINs, you can enter any of these TINs and an NPI associated with the ESCO in that TIN

Organization Type	Required Information	Additional Context
	✓ The National Provider Identifier (NPI) of a clinician in the practice associated with the Organization Site	
APM Entity - OCM	✓ APM Entity ID (your OCM ID) ✓ The Taxpayer Identification Number (TIN) of a practice associated with the Organization Site ✓ The National Provider Identifier (NPI) of a clinician in the practice associated with the Organization Site	If your Practice Site includes multiple TINs, you can enter any of these TINs and an NPI associated with the Practice Site in that TIN
Registry *(Including Qualified Registries and QCDRs)*	✓ The Taxpayer Identification Number (TIN) of the registry or QCDR ✓ Your Vendor ID	CMS issued your Vendor ID when your self-nomination was approved **Note**: You can only connect to a Registry organization that has already been approved by CMS. You don't need to connect to a Registry organization to complete self-nomination for a new entity (i.e. the entity was not approved for a previous performance period).
Virtual Group	✓ The Taxpayer Identification Number (TIN) of two practices participating in the virtual group	

Additional Security Officials and Staff Users

<table>
<tr><th>Additional Security Official</th><th>Staff User</th></tr>
<tr><td>If there is already a Security Official at your organization, select Security Official and click Submit. You will not be prompted to provide additional information.</td><td>If you are a Staff User, select Staff User and click Submit. You will not be prompted to provide additional information.</td></tr>
<tr><td>


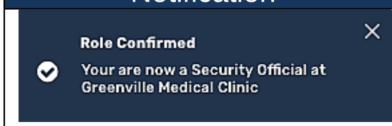
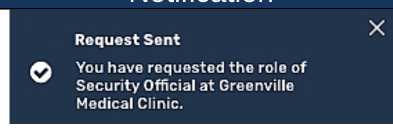
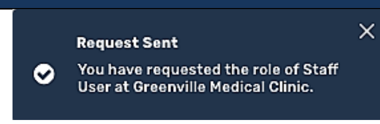
</td><td>


</td></tr>
<tr><th colspan="2">What's Next?</th></tr>
<tr><td>Your Security Official role request is currently pending approval.</td><td>Your Staff User role request is currently pending approval.</td></tr>
</table>

Role Confirmation: Pending or Automatic Approval

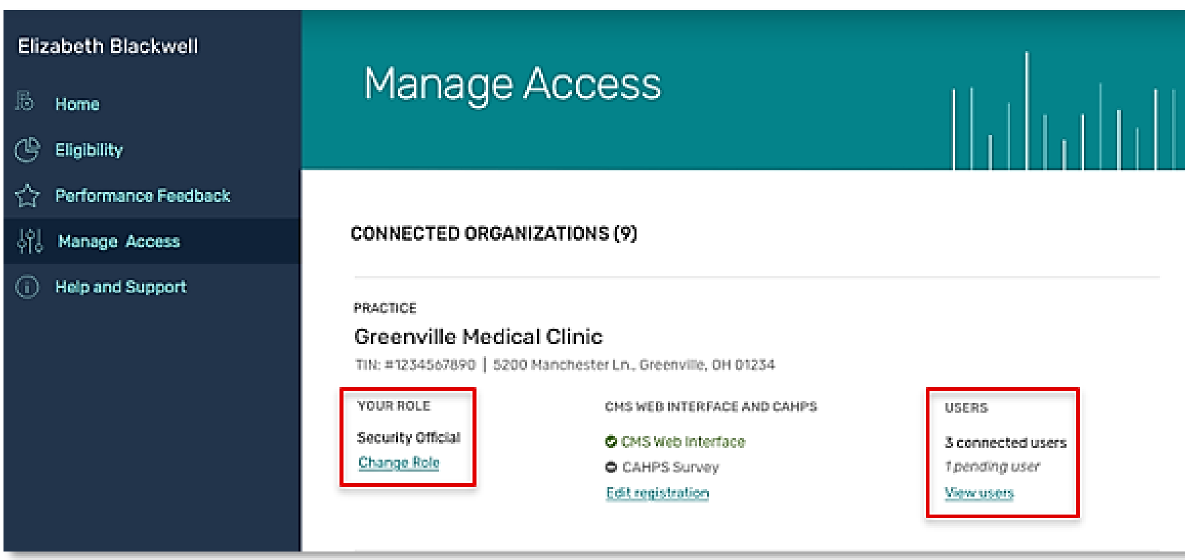
Once you have completed your role selection, you will be redirected to the **Manage Access** page within [qpp.cms.gov](qpp.cms.gov), to **review** your confirmed or pending role requests.

You will receive a **notification** on the screen that displays the state of your request as well as an **email notification**.

First Security Official Notification	Additional Security Official Notification	Staff User Notification
		
Note: The notification example images featured above are for the practice organization type. All organization types will receive similar notifications for their organization type.		

Role Confirmation: Security Official Automatic Approval

If you are the **first** Security Official, you will be **automatically approved** after the required information you provide is validated.

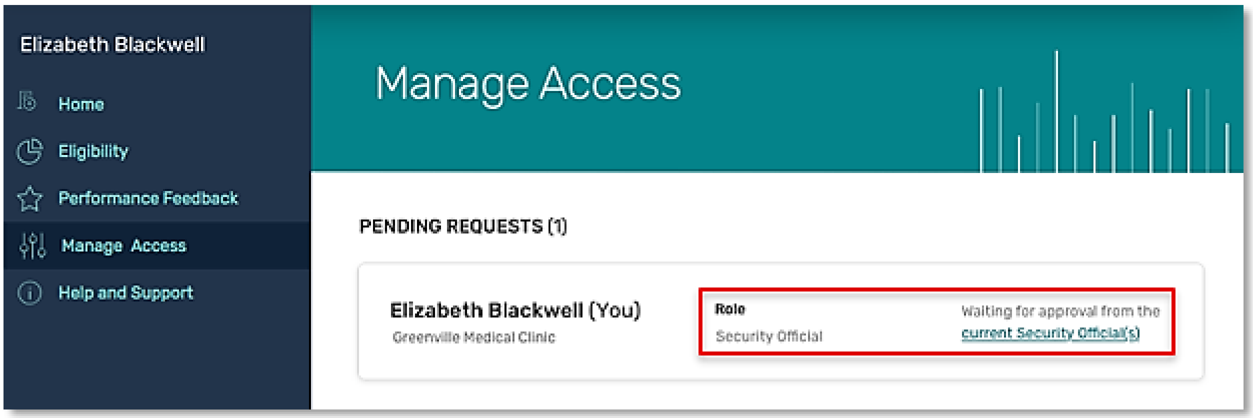


You will **approve pending role requests** from other users requesting access to the practice.

For more information on how to approve other users in your organization, refer to the **Security Officials: Manage Access document** in this guide.

Role Confirmation: Additional Security Officials and Staff Users Pending Approval

If you are an additional Security Official or Staff User, your request will be **pending** and sent to the current Security Official at your organization for approval.



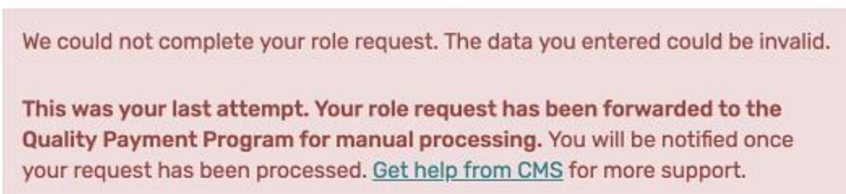
Need to find your organization's Security Official(s) or remove a Security Official?

Contact the Quality Payment Program using the information at the bottom of this page.

Error Messages

If you receive an **error message** while connecting to your organization and selecting a role, please verify and re-enter the required information. If the issue persists, **contact** the Quality Payment Program for further assistance using the contact information at the bottom of each page of this document.

If you receive an error message while requesting a **Security Offical Role**, you will receive an error message indicating that we could **not complete** your role request and that you may have entered **invalid data**. You have **three attempts** to provide valid information to complete your role request. If you are unable to validate your request (image below), your account will be blocked from submitting additional attempts and we will **manually** review your role request.



- If your account is blocked due to failed validation attempts, we will receive notification of your request for the Security Official Role and will automatically generate a QPP Help Desk ticket (i.e. CS00000000) for you regarding your request.
- Once we process your role request, you will be notified via your QPP Help Desk ticket that your request has been processed.
- If you have questions, contact the Quality Payment Program for further assistance using the contact information at the bottom of each page of this document.

Next Steps

- Repeat these steps as needed to connect to additional organizations.
- **Approved Security Officials** will need to monitor for pending requests from other users requesting access to organization(s) in their Manage Access page.
- Staff Users and additional Security Officials will receive an **email notification** when their request has been approved.
- Follow up with **your organization's current Security Official** if you have concerns with the length of time it's taking for your request to be approved. Instructions on how to do so are available here.
- Review the frequently asked questions (FAQs).

Frequently Asked Questions

General

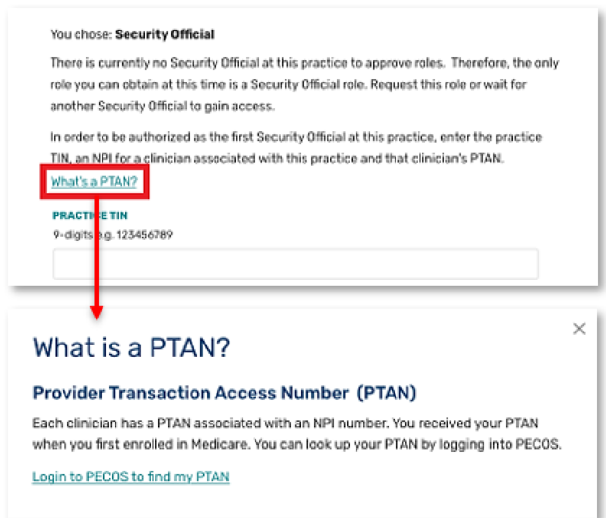
1. I can't find my practice when I search for it. What should I do?

Try changing your search criterion – for example, perform a new search using Legal Business Name instead of Taxpayer Identification Number (TIN), or vice versa. If that doesn't work, contact the Quality Payment Program using the contact information at the bottom of this page. Please note that practice information comes from PECOS, and qpp.cms.gov receives PECOS updates three times per year.

2. What is a PTAN and how do I find it?

Each clinician or provider has a Provider Transaction Access Number (PTAN), associated with their NPI; it was issued at the time of Medicare enrollment and can be found in PECOS.

1. Log into Internet-based PECOS.
2. Select **My Associates** on PECOS home page.
3. Select **View Enrollments** by applicable individual or organizational enrollment.
4. Click on **View Medicare ID Report**
5. PTAN(s) are listed in Medicare ID column.



The first Security Official in the practice will need to provide the PTAN associated with an NPI in the practice. Click the **What is a PTAN** link from Step 3: Select a Role for a link to PECOS.

3. Who do I contact to approve my pending role request?

The first Security Official for an organization will be automatically approved when they can provide the required validation information. Once there's a Security Official at your organization, that individual (and all additional security officials) are responsible for approving all subsequent requests.

If you requested Security Official or Staff User access and awaiting approval from the current Security Official, you may need to reach out to your organization's Security Official. If you don't know who your organization's Security Official is, you can contact the Quality Payment Program (using the information at the bottom of this page) for assistance.

4. **What do I do if the information I provided for my Security Official role request could not be validated?**

   If you receive a validation error message, please verify and re-enter the required information. If the issue persists, contact the Quality Payment Program for further assistance using the contact information at the bottom of each page of this document.

5. **What do I do if a Security Official has left my organization?**

   You can contact the Quality Payment Program using the information at the bottom of this page to have a Security Official removed if they have left your organization.

6. **What do I do if the current Security Official denied my role request?**

   If you believe your request was denied in error, you can submit another request. If you are a clinician, you can also request the **Clinician role** (more information available in this guide), which doesn't require approval by a Security Official.

7. **How can I change my role for an organization?**

   If you need to update your access from Security Official to Staff User (or vice versa), please contact the Quality Payment Program for assistance using the contact information at bottom of each page of this document.

8. **Our CPC+, ESCO, or OCM Practice Site includes multiple TINs, and I will be the first Security Official. Does it matter which TIN and NPI that I enter for verification?**

   No, you can provide any TIN/NPI combination that's associated with your CPC+ Practice Site ID, OCM Practice Site ID or ESCO ID.

Data Submission

Note: Data submission FAQs are updated at the end of each calendar year. Please check the version history table at the end of this document for more information.

9. **A third party is submitting my data for me. Do I need to do anything?**

   We strongly encourage clinicians and representatives of a group, virtual group or APM Entity to sign in to qpp.cms.gov during the submission period and verify the data submitted on their behalf. This will allow clinicians and practice representatives to work with the third party to correct any errors before the submission period closes. Data submission errors found after the submission period closes cannot be corrected.

10. **We are an Electronic Health Record (or other Health IT) vendor. What do we need to do?**

    You will need to complete the Connect to an Organization process for each practice, virtual group or APM entity you represent.

11. **We participate in a Shared Savings Program ACO. What do we need to do?**

Shared Savings Program ACOs (all tracks) must submit their Quality data at the ACO (APM Entity) level.

- A representative of the Shared Saving Program APM Entity will need to be able to sign in to qpp.cms.gov so that they can submit Quality data through the CMS Web Interface at the ACO level. This representative will choose **APM Entity** as the organization type, Shared Savings Program as the model, and request the Staff User or Security Official role. Each ACO must have a Security Official before anyone can request a Staff User role or additional Security Official roles.

Practices participating in the Shared Savings Program must submit their Promoting Interoperability data at the group (Practice) level.

- A representative of your practice (i.e. a single TIN participating in the larger ACO entity) will need to be able to sign in to qpp.cms.gov to submit this Promoting Interoperability data at the group level or view data submitted on your behalf by a third party. The representative should choose **Practice** as the organization type and request the Staff User or Security Official role.

12. We participate in the Shared Savings Program and CPC+. What do we need to do?

Shared Savings Program ACOs (all tracks) must submit their Quality data at the ACO (APM Entity) level.

- A representative of the Shared Saving Program APM Entity will need to be able to sign in to qpp.cms.gov so that they can submit Quality data through the CMS Web Interface at the ACO level. This representative will choose **APM Entity** as the organization type, Shared Savings Program as the model, and request the Staff User or Security Official role.

Practices participating in the Shared Savings Program must submit their Promoting Interoperability data at the group (Practice) level.

- A representative of your practice (i.e. a single TIN participating in the larger ACO entity) will need to be able to sign in to qpp.cms.gov to submit this Promoting Interoperability data at the group level or view data submitted on your behalf by a third party. The representative should choose **Practice** as the organization type and request the Staff User or Security Official role.

CPC+ practices must submit their Quality data at the Practice Site (APM Entity) level.

- A representative of the CPC+ APM Entity will need to be able to sign in to qpp.cms.gov so that they can submit data for the Quality performance category at the ACO level. This representative will choose **APM Entity** as the organization type, CPC+ as the model, and request the Staff User or Security Official role.

13. **Our virtual group includes clinicians in a MIPS APM. What do we need to do?**

The virtual group only has the responsibility of meeting the reporting requirements for the virtual group. The virtual group's submission will not satisfy any reporting requirements for MIPS APM participation or MIPS scoring under the APM scoring standard.
The virtual group needs to aggregate and submit data for all clinicians within the virtual group for the Quality, Promoting Interoperability and Improvement Activities performance categories just like any other virtual group.

- The virtual group will need to be able to sign in to qpp.cms.gov to submit their data or view data submitted on behalf of the virtual group by a third party. (See Connect to a Virtual Group.)

Clinicians participating in a virtual group do not need to submit data outside of the virtual group at the individual or group level to meet virtual group reporting requirements.
Please refer to this FAQ for more information on the roles and access needed for MIPS APM data submission.

14. **Our practice participates in a MIPS APM and our clinicians are scored under the APM scoring standard. What do we need to do?**

You will need to complete the Connect to an Organization process, selecting **Practice** as the organization type, in order to submit any individual or group-level data necessary for your MIPS APM participation, such as Promoting Interoperability measure data. (See Connect to a Practice.)
For MIPS APM participation, **the APM Entity** will submit Quality data on behalf of all eligible clinicians in the APM Entity group.

- Medicare Shared Savings Program ACOs, Next Generation ACOs, and CPC+ practices will need to be able to sign in to qpp.cms.gov to submit Quality data on behalf of the APM Entity or view data submitted on their behalf by a third party. (See Connect to an APM Entity)

15. **We are a single TIN ACO. How will we submit our Quality data at the entity level and our Promoting Interoperability data at the group level?**

Because you will need access to your organization as both a **Practice** and an **APM Entity**, you will need to complete the Connect to an Organization process **twice** – one time selecting **Practice** as your organization type, and a second time selecting **APM Entity** as your organization type.
Additionally, CMS has a list of single TIN ACO organizations, which will allow the first Security Official requesting the APM Entity access to complete the request by providing a single TIN for verification.

If you are an existing user with EIDM credentials associated with a single TIN ACO, you should see your organization listed both as an **APM Entity** and as a **Practice** on the **Manage Access** page.

Version History

Date	Description of change
12/18/18	Original posting
07/01/19	The guide was restructured to shorten it, and new content was added: • Updated title to indicate role selection process (select a role) • CEC and OCM information (these models can now get acess to their entity) • Clinician role references (new document that outlines this new role) • Role needed for self-nomination (existing Qualified Registries/QCDRs only)