

# **Provider Portal: Provider Organization User Guide**

California Medicaid Management Information System

V 1.9

March 2026

# Table of Contents

<b>Introduction to the Provider Portal</b> .....	<b>1</b>
<b>Provider Dashboard</b> .....	<b>2</b>
<b>Register and Add An Organization</b> .....	<b>4</b>
Set A Passkey .....	11
One-Time Passcode .....	11
Select An Organization .....	12
Switch Organizations and NPIs .....	13
Add An Enrolled Provider Organization .....	15
<b>NPI Agreements and Settings</b> .....	<b>16</b>
PIN Management .....	16
Transactions Available .....	18
Presumptive Eligibility Provider Agreements .....	19
<b>Manage Users</b> .....	<b>19</b>
Add a User .....	20
User Contact Information .....	22
User Permissions .....	22
NPI Permissions .....	23
Quick Assign to All NPIs .....	24
Correspondence Permissions .....	25
NPI Level Correspondence Permissions .....	28
Permissions Across Organization .....	31
Reactivate User .....	33
Unlock An Account .....	35
Reset Password .....	37
Forgotten Password at Login .....	38
Domain Management .....	41
<b>Submitter Management</b> .....	<b>42</b>
New Affiliation Request to a Submitter Organization .....	44
Approve a Submitter Affiliation Request .....	47
Deny a Submitter Affiliation Request .....	47
Manage Submitters .....	48
Submitter Directory .....	53

<b>Navigating the Provider Portal .....</b>	<b>54</b>
My Account .....	54
Profile .....	55
NPI Preferences .....	57
Email Notification Preferences .....	57
Going Paperless .....	58
Edit Tax Document Enrollment .....	59
Guided Tours .....	61
Organizations .....	62
Transaction Center .....	62
Correspondence Center .....	64
Types of Correspondence .....	65
Message Center .....	70
Edit Email Notification Preferences .....	70
<b>Change Summary .....</b>	<b>73</b>

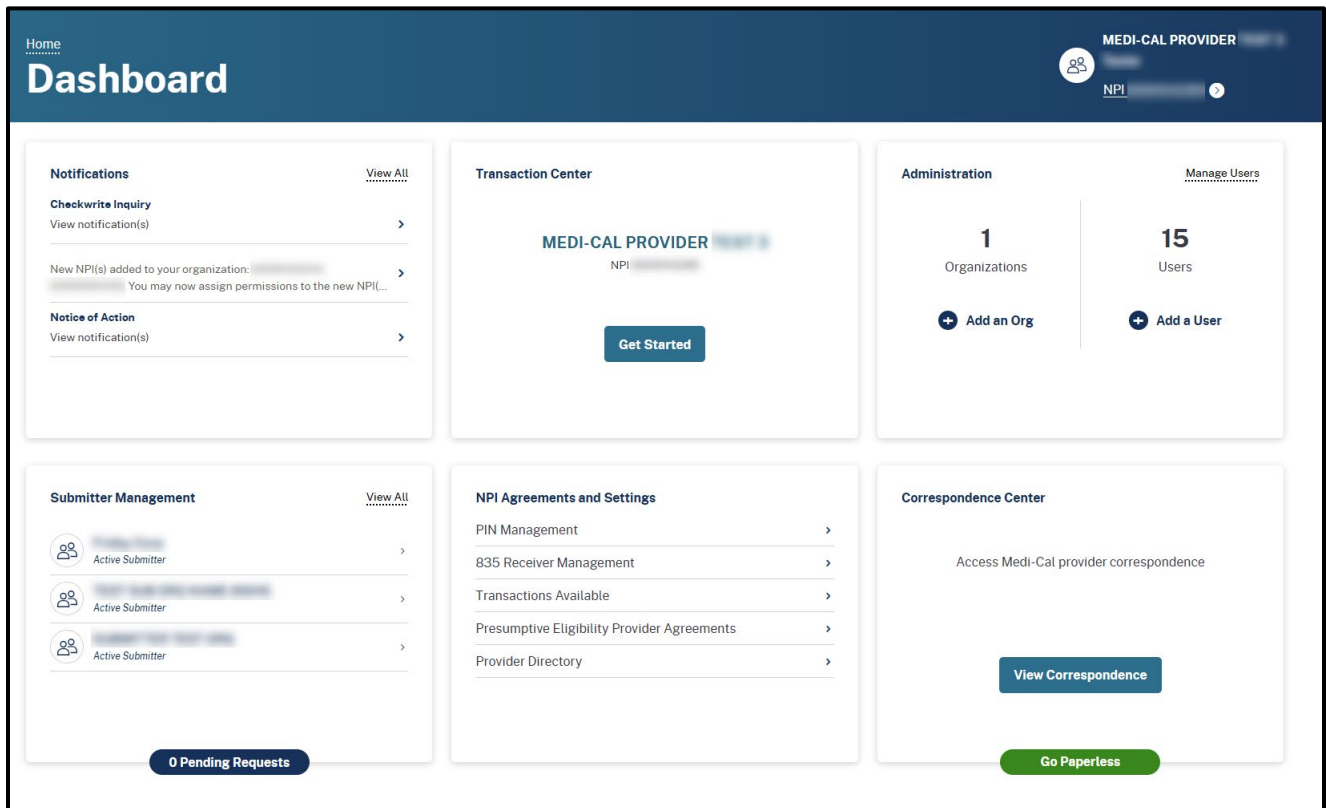
# Introduction to the Provider Portal

The Provider Portal is an area within the Medi-Cal Providers website that houses general information and day-to-day work for Medi-Cal providers and provider healthcare staff. It focuses on reducing paper communication increasing the security and accessibility of Medi-Cal electronic services and empowering Provider Portal users to administer their own organization within the Portal. The Provider Portal allows providers and submitters to:

- Perform billing work for multiple National Provider Identifiers (NPIs) with a single administrative account
- Interact with Medi-Cal more seamlessly
- Go Paperless
- Access correspondence based on NPI access in the Correspondence Center
- Instantly receive correspondence, instead of waiting for traditional mail, and quickly resolve issues
- Access fee-for-service 1099 forms electronically for all NPIs who have received reimbursement a few weeks earlier than traditional mail
- Perform self-service capabilities, such as password and NPI Provider Identification Number (PIN) reset
- Complete provider-submitter affiliations electronically
- Test Eligibility Benefit 270/271 transactions

# Provider Dashboard

The Provider Portal provides access to provider transactions and house communications, notifications, and organization information. Users within an organization can be assigned as either an Administrator or a Processor. The **Dashboard** is the home page of the Provider Portal.



**Figure 1.1:** Provider Admin Dashboard.

The portal contains six (6) areas on the **Dashboard**. Detailed information about each can be found later in this user guide. Here is an overview:

- The **Notifications** tile allows a user to view unread and past notifications about an organization. Notifications can be searched for or filtered by date.
- The **Transactions Center** tile allows a user to create and keep track of various transactions and single sign on to Transaction Services.

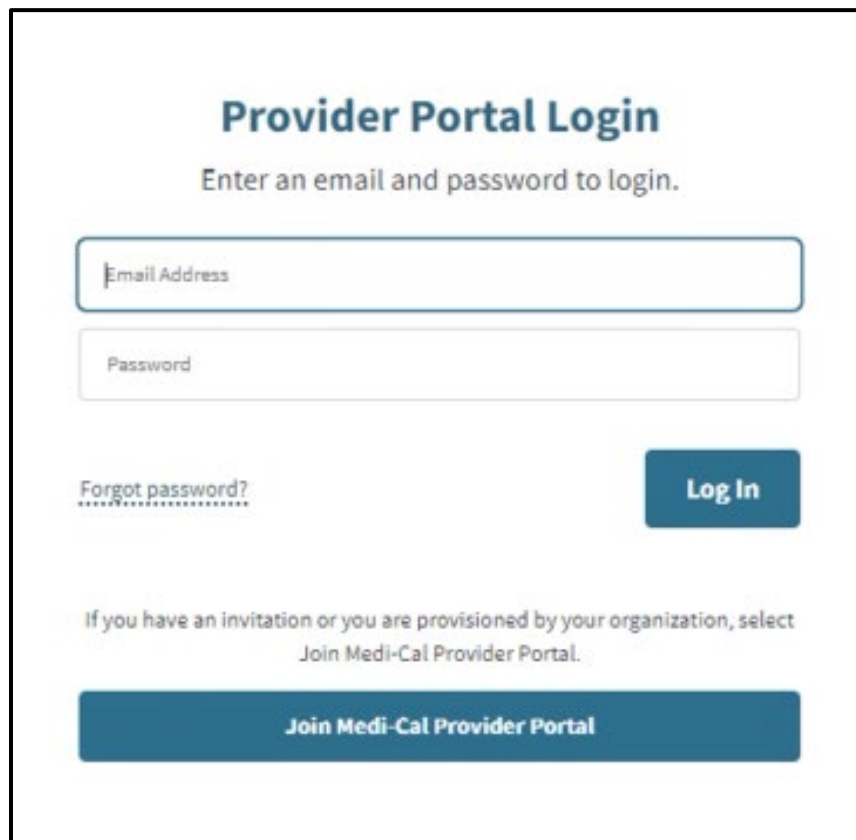
- The **Administration** tile displays information about users within an organization. This area permits Administrators to: update user permissions and information, to add and/or remove user profiles.
- The **Submitter Management** tile allows a user to view new affiliation and pending requests, manage submitters and view the submitter directory.
- The **NPI Agreements and Settings** tile allows a user to search for NPIs within an organization, update NPI Provider Identification Numbers (PINs) and manage 835 receivers, Transactions Available and Presumptive Eligibility Provider Agreements.
- The **Correspondence Center** tile allows a user to electronically search, view and download correspondence related to the organization.

# Register and Add An Organization

This is the first step for an organization to set up the Provider Portal and should be completed by one individual. This person will automatically be given the role of Administrator in the Provider Portal and includes permissions for all NPIs and correspondence. Additional users may be assigned as an Administrator or a Processor. An Administrator will have access to all Provider Portal features and organization administration functions. The Processor can use features such as Transaction Testing and certain applications but will not have access to the organization's administration functions.

After registering an organization, DHCS will issue a one-time registration token to the provider. This token will be sent by hard copy (paper) to the pay-to address on file with Medi-Cal. **It must be used within 30 days of the date it is issued or it will expire.** Once the Administrator has been selected and has received the token, these steps should be followed:

1. Navigate to the **Log In** screen and select **Join Medi-Cal Provider Portal**.



**Provider Portal Login**  
Enter an email and password to login.

Email Address

Password

Forgot password?

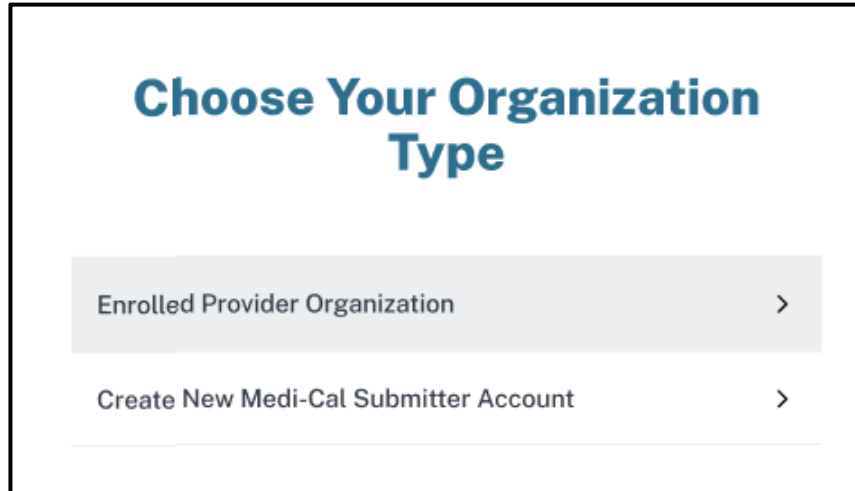
Log In

If you have an invitation or you are provisioned by your organization, select  
Join Medi-Cal Provider Portal.

Join Medi-Cal Provider Portal

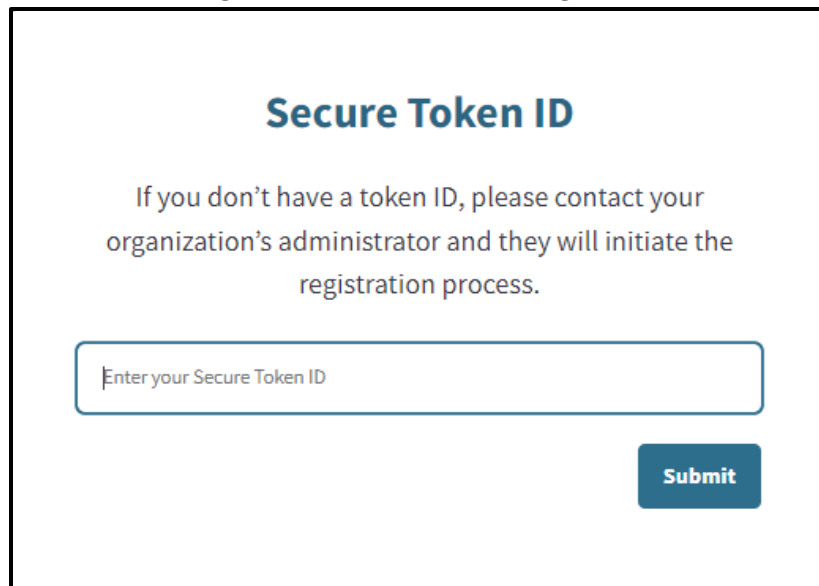
**Figure 2.1:** Join Medi-Cal Provider Portal Log In.

2. A **Choose Your Organization Type** screen will appear. Select **Enrolled Provider Organization**.



**Figure 2.2:** Choose Organization Type.

3. The **Secure Token ID** pop-up window appears. Enter the unique token and select **Submit**. The Terms and Conditions for the Medi-Cal Provider Portal window displays.



**Figure 2.3:** Secure Token ID.

4. Read the terms and conditions and select “I confirm that I have read and agree to the above” and “I confirm that I am authorized to create a Medi-Cal Provider Portal account of behalf of my organization.”
5. Check the confirmation boxes then select **Next**.

## Terms and Conditions for Medi-Cal Portal

Welcome to the Medi-Cal Provider Portal. Please read and agree to the Terms and Conditions to proceed to the portal.

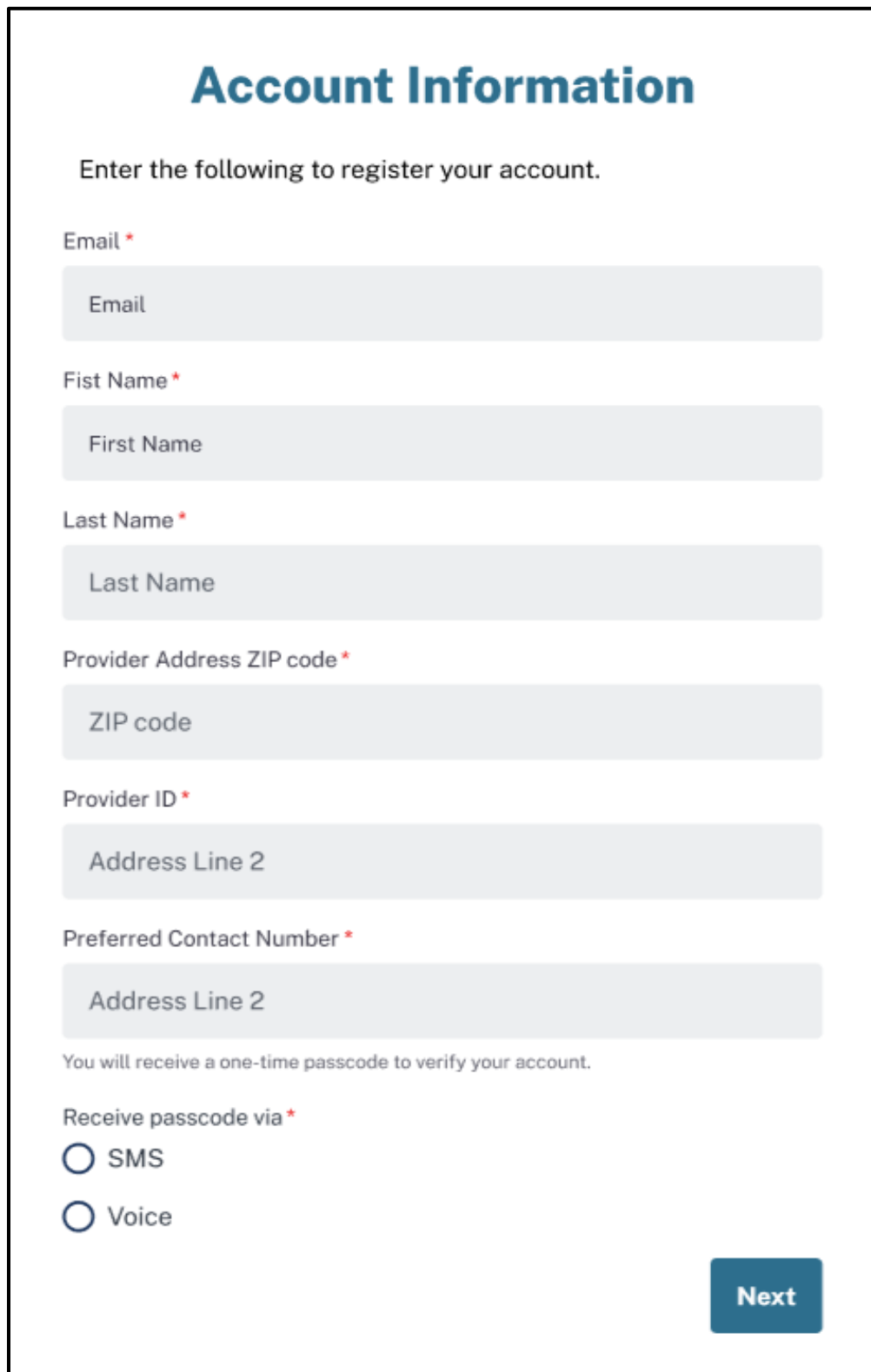
**WARNING:** This computer system is for official use by authorized users and may be monitored and/or restricted at any time. Confidential information may not be accessed or used without authorization. Unauthorized or improper use of this system may result in administrative discipline, civil and/or criminal penalties. By using this system, you are acknowledging and consenting to these terms and conditions.

**LOG OFF IMMEDIATELY** if you are not an authorized user or do not agree to the conditions in this warning.

- I confirm that I have read and agree to the above
- I confirm that I am authorized to create a Medi-Cal Provider Portal account of behalf of my organization.

**Figure 2.4:** Terms and Conditions for Medi-Cal Portal.

6. Enter the required information and select **Next**.



**Account Information**

Enter the following to register your account.

Email \*

Email

First Name \*

First Name

Last Name \*

Last Name

Provider Address ZIP code \*

ZIP code

Provider ID \*

Address Line 2

Preferred Contact Number \*

Address Line 2

You will receive a one-time passcode to verify your account.

Receive passcode via \*

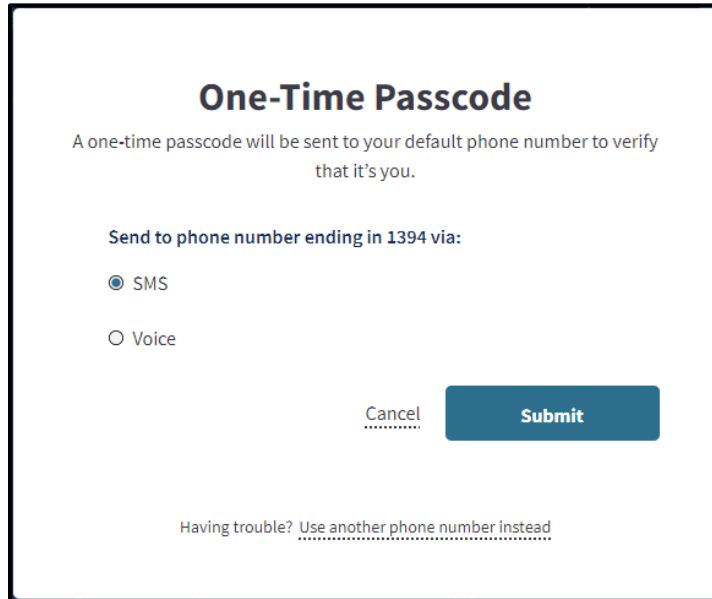
SMS

Voice

**Next**

**Figure 2.5:** Account Information.

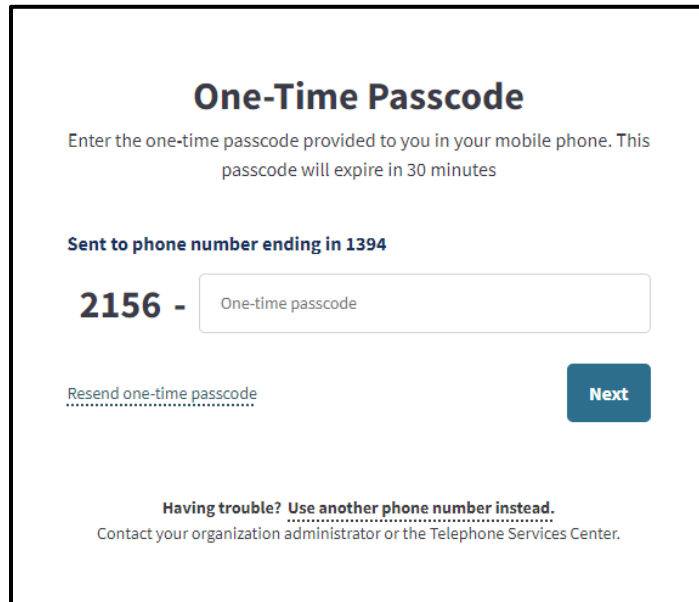
7. To verify the account, a One-Time Passcode (OTP) will be sent to the Administrator's phone. The Administrator will need to indicate how to receive this passcode, via SMS (text) or Voice (call). Select the method and select **Submit**.



The screenshot shows a mobile application screen titled "One-Time Passcode". Below the title, it says "A one-time passcode will be sent to your default phone number to verify that it's you." There are two radio button options: "SMS" (which is selected) and "Voice". At the bottom right, there are two buttons: "Cancel" and "Submit". At the bottom center, there is a link that says "Having trouble? Use another phone number instead".

**Figure 2.6:** One-Time Passcode.

8. A screen for entering the OTP appears. Enter the last six digits of the code and select **Next**.

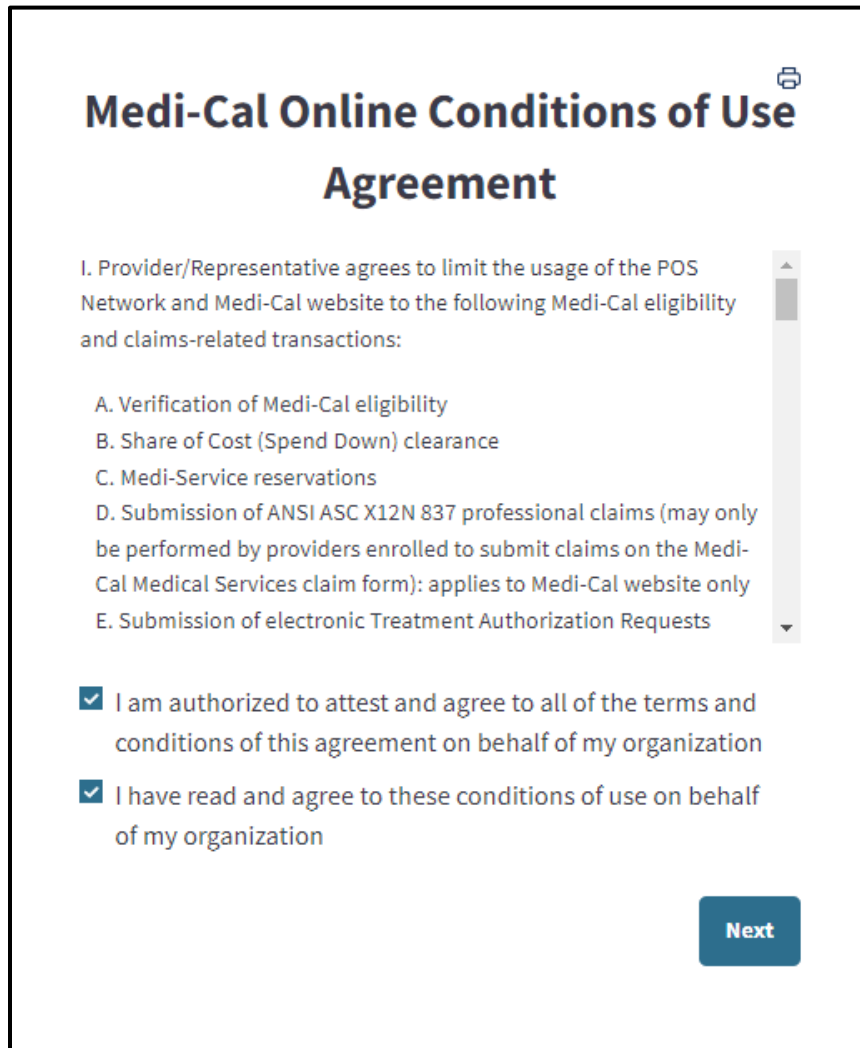


The screenshot shows a mobile application screen titled "One-Time Passcode". Below the title, it says "Enter the one-time passcode provided to you in your mobile phone. This passcode will expire in 30 minutes". There is a line of text "Sent to phone number ending in 1394" followed by "2156 -" and a text input field containing "One-time passcode". Below the input field, there is a link "Resend one-time passcode" and a "Next" button. At the bottom, there is a link "Having trouble? Use another phone number instead." and a note "Contact your organization administrator or the Telephone Services Center."

**Figure 2.7:** Enter the OTP.

9. Read the **Medi-Cal Online Conditions of Use Agreement**.

10. Check the required boxes and select **Next**.



The screenshot shows a web form titled "Medi-Cal Online Conditions of Use Agreement". At the top right of the title is a printer icon. Below the title, there is a list of conditions (I through E) and two checked checkboxes. A vertical scrollbar is on the right side of the list. At the bottom right is a blue "Next" button.

## Medi-Cal Online Conditions of Use Agreement

I. Provider/Representative agrees to limit the usage of the POS Network and Medi-Cal website to the following Medi-Cal eligibility and claims-related transactions:

- A. Verification of Medi-Cal eligibility
- B. Share of Cost (Spend Down) clearance
- C. Medi-Service reservations
- D. Submission of ANSI ASC X12N 837 professional claims (may only be performed by providers enrolled to submit claims on the Medi-Cal Medical Services claim form): applies to Medi-Cal website only
- E. Submission of electronic Treatment Authorization Requests

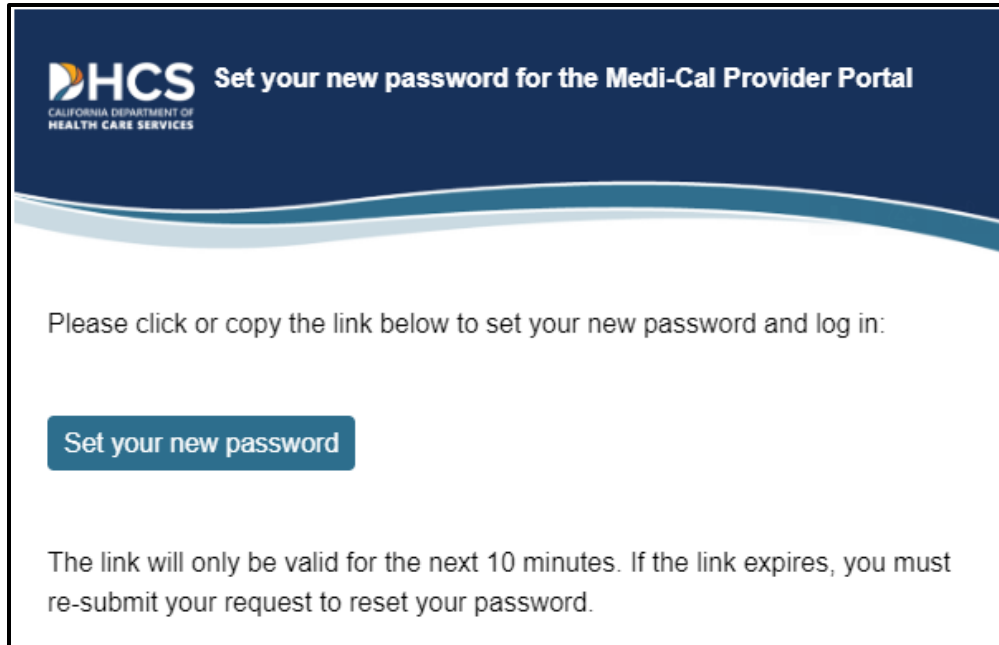
I am authorized to attest and agree to all of the terms and conditions of this agreement on behalf of my organization

I have read and agree to these conditions of use on behalf of my organization

**Next**

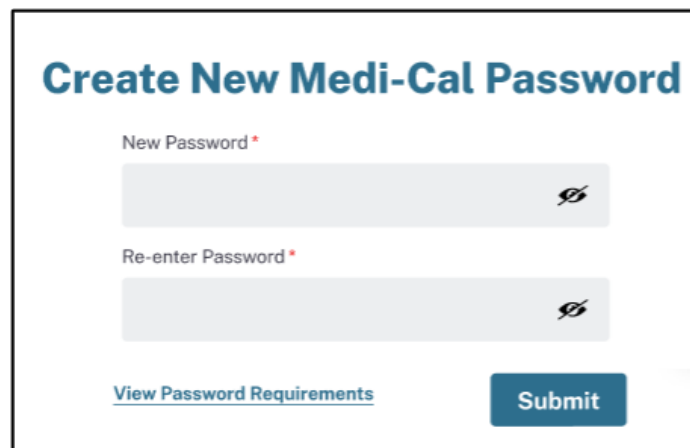
**Figure 2.8:** Medi-Cal Online Conditions of Use Agreement.

11. An email will be sent to the address indicated during sign-up to set up a password. Select **Set your new password** to continue the registration process. **This must be done within 10 minutes, or the link will expire.** If this process is not completed within the 10 minutes, the Administrator may initiate a password reset with the email used during registration to gain access to the portal.



**Figure 2.9:** Set new password email notification.

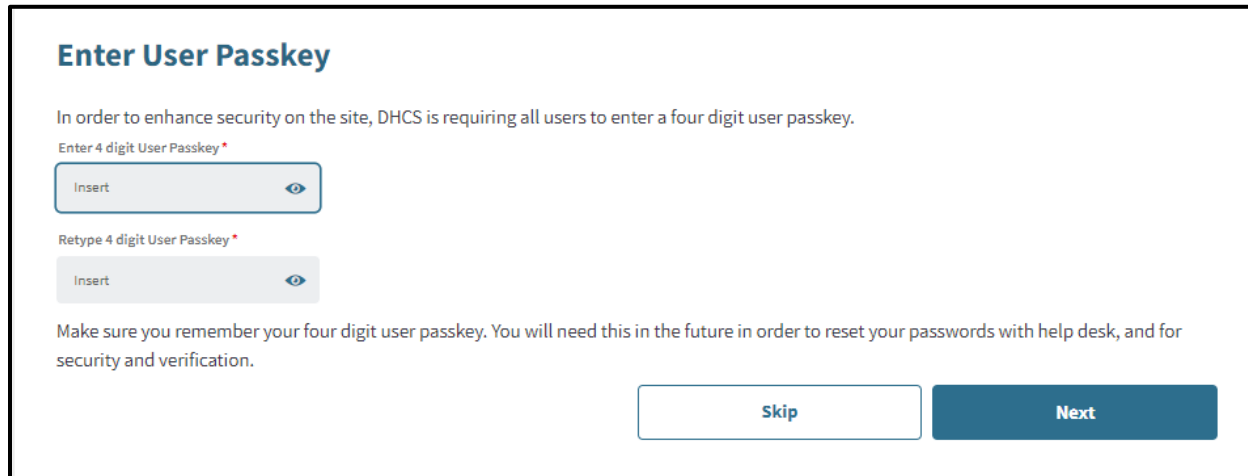
12. A pop-up window to create a new password will appear. The password must be a minimum of 15 characters and contain at least one uppercase letter, one lowercase letter, one numeral and one special character. A previous password cannot be reused. Enter a password that aligns with the password criteria and select **Submit**. The Administrator has now successfully registered with the organization and has administrative privileges to all NPIs in the organization.

The image shows a web form titled "Create New Medi-Cal Password". It has two input fields: "New Password \*" and "Re-enter Password \*", both with a strength indicator icon on the right. Below the fields is a link "View Password Requirements" and a blue "Submit" button.

**Figure 2.10:** Create New Medi-Cal Password.

# Set A Passkey


After registration is complete, the **Enter User Passkey** page will appear to create a four-digit passkey for additional security. Once the new passkey is entered select **Next** to continue or select **Skip** to bypass adding the new passkey. The passkey may be set later from the **My Account** tab of the dashboard.




**Enter User Passkey**

In order to enhance security on the site, DHCS is requiring all users to enter a four digit user passkey.

Enter 4 digit User Passkey \*

Insert 

Retype 4 digit User Passkey \*

Insert 

Make sure you remember your four digit user passkey. You will need this in the future in order to reset your passwords with help desk, and for security and verification.

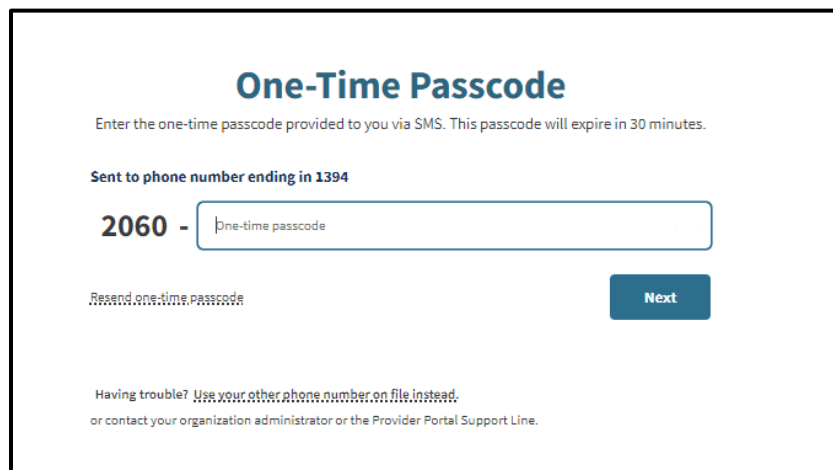
[Skip](#) [Next](#)

**Figure 2.11:** Enter User Passkey.

# One-Time Passcode

The Provider Portal uses a two-factor authentication to ensure security. At any time while conducting business in the Portal, a **One-Time Passcode** pop-up will appear. If the pop-up appears, a code will automatically be sent to the user’s phone either by SMS, text or voice depending on how the user configured the settings. Enter the passcode and select **Next** to continue in Portal.

**Note:** To edit phone settings, refer to “Editing Phone Number” section in this user guide.



**One-Time Passcode**

Enter the one-time passcode provided to you via SMS. This passcode will expire in 30 minutes.

Sent to phone number ending in 1394

2060 -

[Resend one-time passcode](#) [Next](#)

Having trouble? [Use your other phone number on file instead.](#)  
or contact your organization administrator or the Provider Portal Support Line.

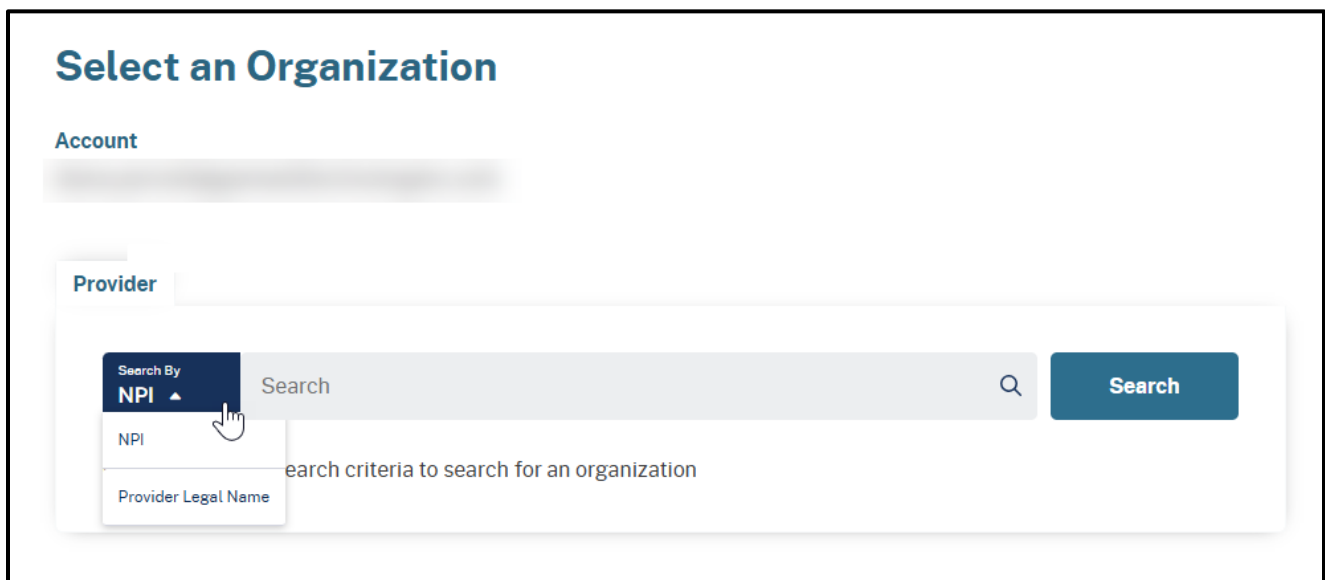
**Figure 2.12:** One-Time Passcode.

# Select An Organization

When the **Select an Organization** webpage appears, it will prompt the Administrator to select an organization. The Administrator can search an organization by the provider's NPI or Provider Legal Name. The organizations displayed are determined by an Administrator when initially adding the user. Refer to the Add a User section of this user guide for instructions.

This view only appears if there are multiple organizations to which the user is assigned. If the user is assigned to a single organization, the Dashboard opens immediately.

1. Select the desired search criteria from the **Search By** drop down then enter the NPI or Provider Legal Name in the search field. Select the **Search** button to submit the query.



**Figure 2.13:** Search for an Organization.

2. Search results are presented in a list. Select the preferred organization. This serves as the default organization. Refer to the Switch Organization section of this user guide for information on changing the default.

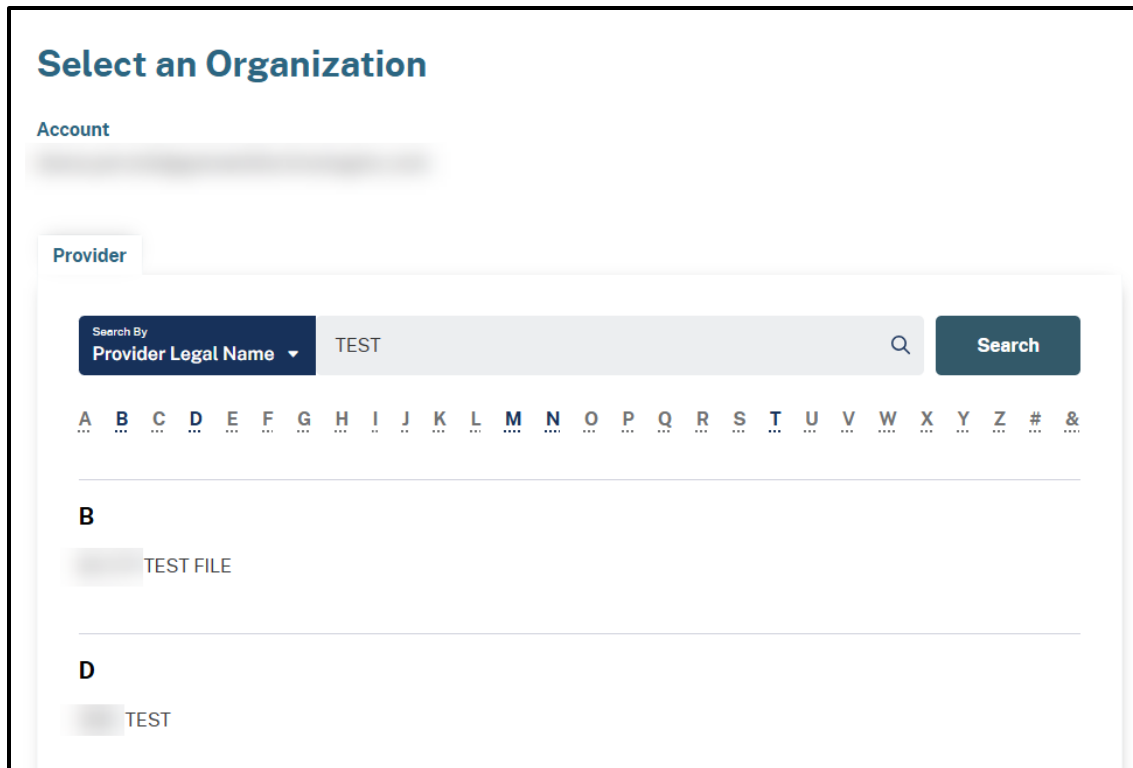


Figure 2.14: Select an Organization.

## Switch Organizations and NPIs

This feature is only available if a user has been granted access to multiple organizations by the organizations' respective Administrator. The current NPI is always visible in the page banner at the top of the screen.

**Note:** Organization and NPI cannot be changed when work is in progress. Work must be saved or exited before changes can be made.

1. If a user wishes to switch to a different organization, the user can do so at any time by selecting the **Organization ID** hyperlink with the “more” (⌵) icon from the top banner.

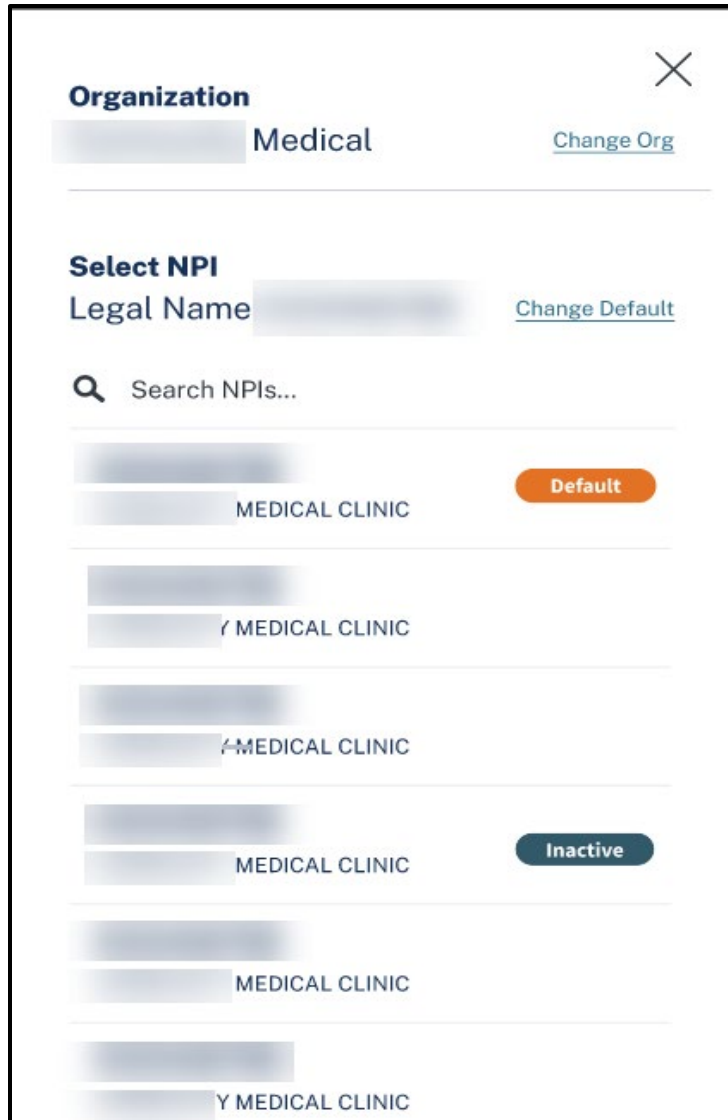


Figure 2.15: Add or Switch Organization.

**Note:** If the “more” (⌵) icon next to the NPI is not visible it indicates there is no access to multiple organizations or NPIs and switching is not allowed.

- The **NPI selector** panel opens. The user can change the default NPI or change or switch organizations by selecting one of the items on the list. The NPI selector panel lists all associated organizations and indicates which is the **Default** and those that are **Inactive**. **Select** an NPI to make it active.

**Note:** The default NPI will automatically be selected at log in to the Portal.



**Figure 2.16:** NPI Selector Panel.

# Add An Enrolled Provider Organization

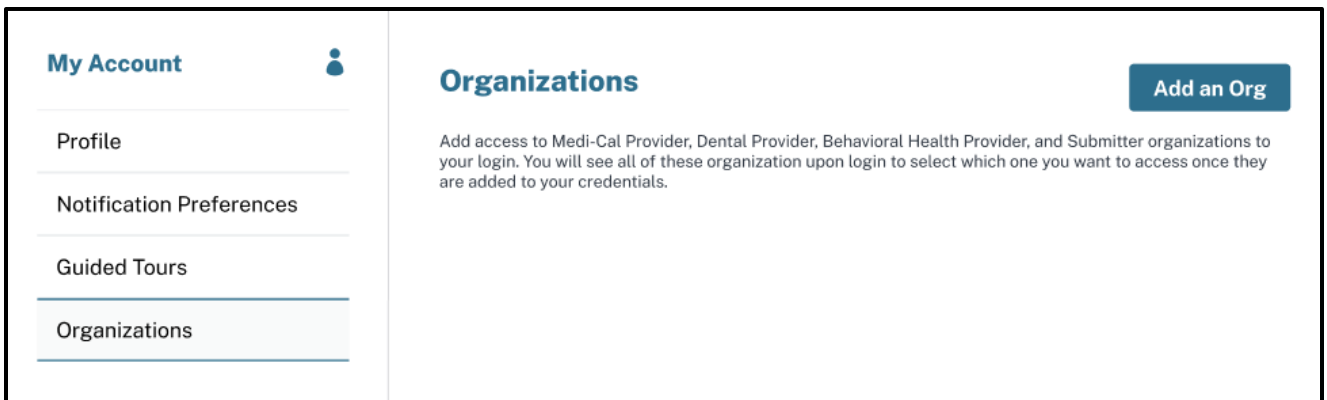
An Organization Administrator can add a new provider or submitter organization at any time in the Provider Portal. Only after an organization is registered and has an account can a new organization be added. Refer to the Register the Organization section in this user guide for more information regarding registering an account for the first time.

1. Select the My **Account** tab from any page in Provider Portal.



**Figure 2.17:** Provider Portal Top Navigation.

1. Select **Add an Org**. Refer to the Register an Organization section of this user guide for step-by-step instructions.



**Figure 2.18:** Add an Organization.

# NPI Agreements and Settings

The **NPI Agreements and Settings** area allows organizations to manage PINs, access available transactions, designate receivers for 835 Transactions and complete the Presumptive Eligibility Provider Agreements.



Figure 3.1: NPI Agreements and Settings Tile.

## PIN Management

1. Either search by Provider Name or NPI or select the NPI from the list provided on the screen.

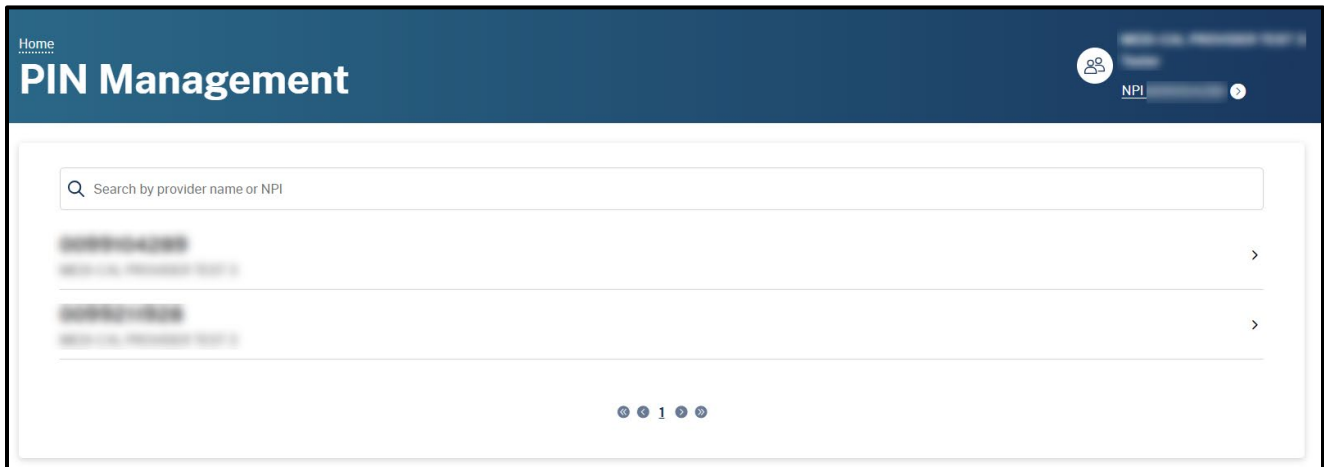
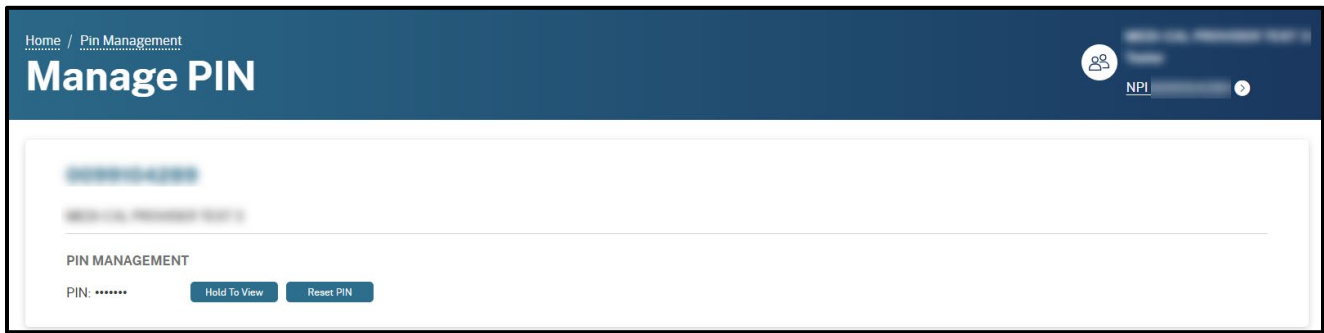


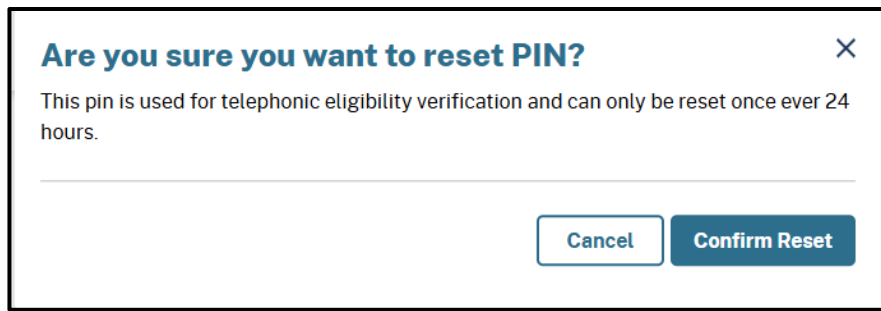
Figure 3.2: Search for NPI.

2. View the current PIN by pressing and holding the **Hold to View** button.



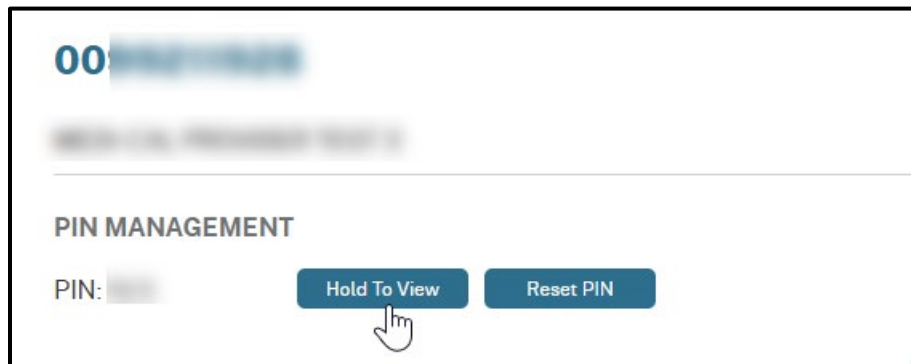
**Figure 3.2:** NPI PIN Details.

3. Select **Reset PIN**
4. Select **Confirm Reset**. The PIN resets to a randomized seven-digit PIN. The action resets the PIN for all users so ensure that any impacted users are notified.



**Figure 3.3:** Confirm PIN Reset.

5. Select **Hold To View** to see the PIN.



**Figure 3.4:** Hold to View.

Refer to the [Medi-Cal Electronic Data Interchange \(EDI\) User Guide](#) for details about managing 835 receivers.

# Transactions Available

Once an NPI is assigned by the Organization Administrator, the user will have access to view the available transactions for the designated NPI.

KING, JUSTIN B MD INC	
NPI	
Transactions	
Claims ^	
Appeal Status Inquiry	(i)
Blood Factor Rates	(i)
Claim Status Inquiry	(i)
Medical Supply Code Inquiry	(i)
Procedure Code Inquiry	(i)
National Drug Code Inquiry	(i)
Current Remittance Advice Detail	(i)
Historical Remittance Advice Detail	(i)
Provider Checkwrite Inquiry	(i)

**Figure 3.5:** NPI Transactions List.

If a transaction is listed with an orange pill, it will indicate what is required to access the transaction link. For example, if an orange pill states, “Testing Required,” the user must complete testing. If the orange pill states, “835 Receiver Required,” it means an 835 receiver is not assigned for the NPI.

EDI Transactions	
Claim Status Request (276)	(i)
Claim Status Response (277)	(i)
Eligibility Benefit Inquiry (270)	Testing Required (i)
Eligibility Benefit Response (271)	Testing Required (i)
Eligibility Benefit Testing (270)	(i)
Health Care Claim Payment/Advice (835)	835 Receiver Required (i)
Electronic Treatment Authorization Request	
eTAR	(i)
eTAR Inquiry	(i)
Medical Services Reservation	(i)
TAR 3 Attachment Form	(i)

**Figure 3.6:** NPI Transactions List Requirement.

# Presumptive Eligibility Provider Agreements

The Presumptive Eligibility Provider Agreements link allows Presumptive Eligibility (PE) providers to access the agreements for Hospital Presumptive Eligibility (HPE) and Presumptive Eligibility for Pregnant People (PE4PP). For more information about the agreements, refer to the [HPE Application User Guide](#) or the [PE4PP Application User Guide](#).



Figure 4.1: Select PE Program Type Drop-Down Menu.

# Manage Users

This area may only be accessed by individuals who are designated as Organization Administrators.

1. Select **Manage Users**.

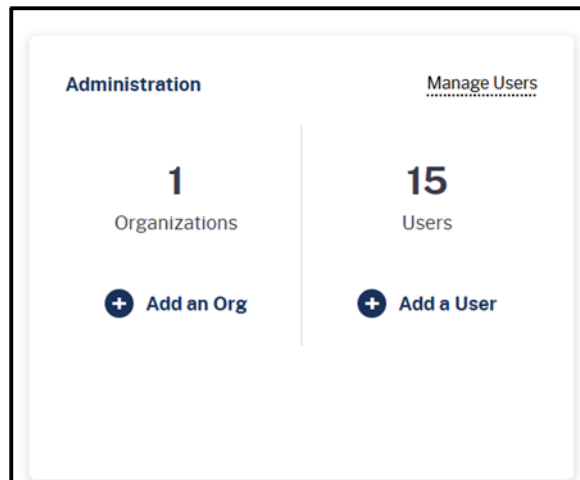


Figure 5.1: Administration Tile.

- The Manage Users page displays the full overview of the Organization’s users, correspondence permissions and domain management. Administrators can identify user status visually with the following icons: (Y) currently active, (N) currently inactive (🔒) locked account and (⚠️) registration link expired. Select a **name** from the list to view the user management and permission details. The full list can also be exported in the following formats: .xls, .csv or .txt.

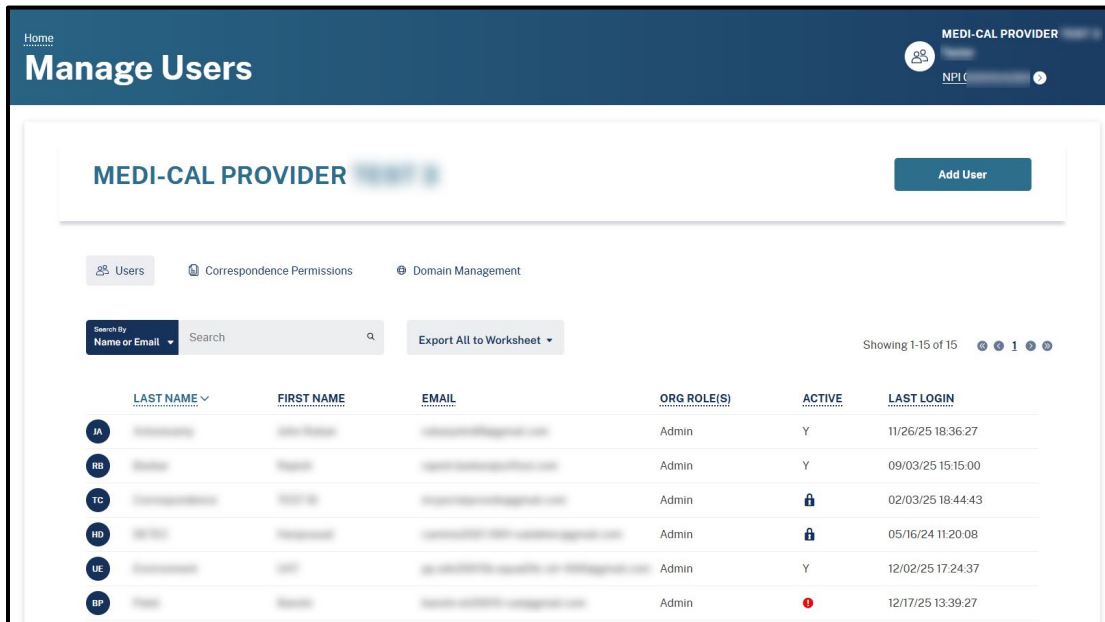


Figure 5.2: Manage Users Webpage.

## Add a User

From the Manage Users page the Administrator can add a user to their organization.

- Select **Add User**.

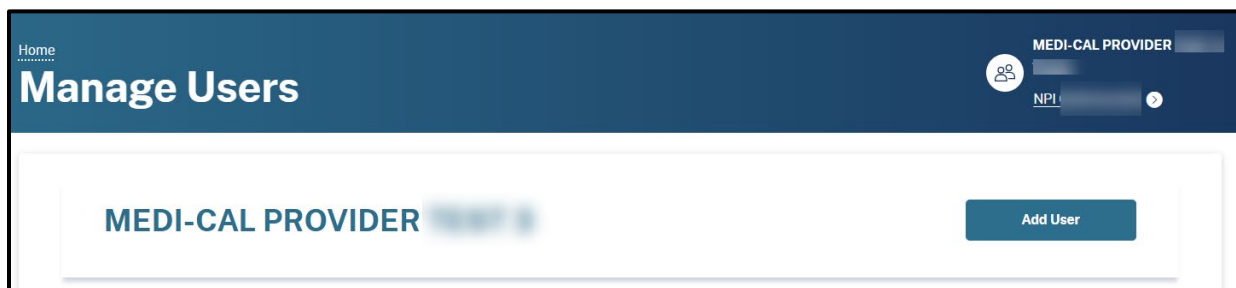
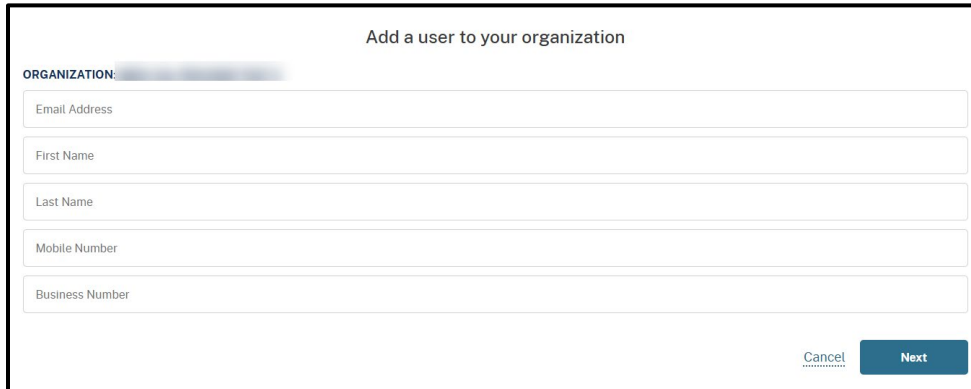


Figure 5.3: Add User In Manage Users Page.

2. Enter the user's **Email Address**, **First Name**, **Last Name**, **Mobile Number** and **Business Number** then select **Next**. If the user only has one phone number, enter the same number for both mobile and business.



Add a user to your organization

ORGANIZATION: [REDACTED]

Email Address

First Name

Last Name

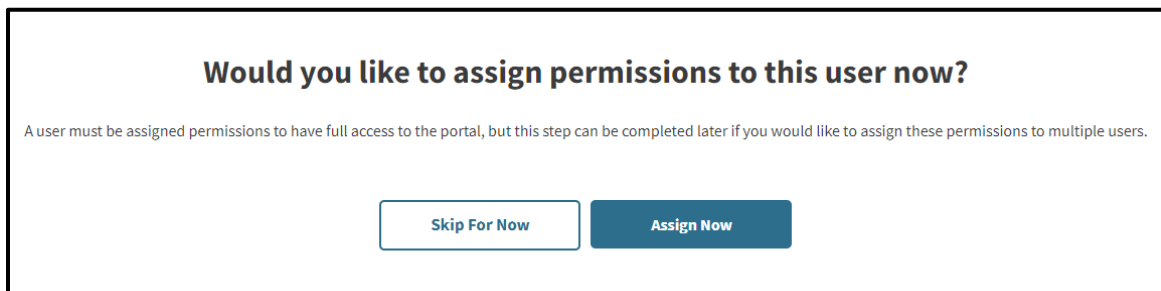
Mobile Number

Business Number

[Cancel](#)

**Figure 5.4:** Add a User.

3. Once the Administrator has added a new user, a unique link to register with the Provider Portal is emailed to the user. This link can only be used once, and it **must be used within seven (7) days**. If it is not used within seven days, the link expires, and the Administrator must initiate a new registration email. The Administrator can choose to set permissions for a new user at any time. Once the user has registered their account, they may log into the account at any time.
3. Select **Assign Now** to proceed with assigning permissions for the user added to the organization. If **Skip For Now** is selected, the user will have very limited access to the organization. Their permissions can be updated at a later time. If permissions are never assigned the user will eventually be deactivated and the Administrator will need to reactivate the user. Refer to the [User Permissions](#) section of this user guide for additional details regarding adding or editing user permissions.



**Would you like to assign permissions to this user now?**

A user must be assigned permissions to have full access to the portal, but this step can be completed later if you would like to assign these permissions to multiple users.

**Figure 5.5:** Assign User Permissions.

# User Contact Information

From the **User Management and Permissions** webpage administrators have full access to update contact information, reactivate or deactivate users, update correspondence permissions and define permissions across organizations.

1. Select **Edit** next to the user contact information that needs updating.

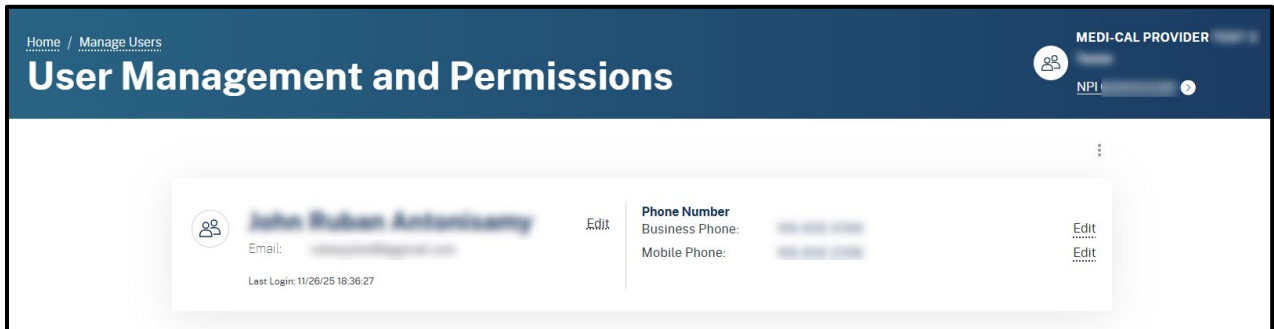


Figure 5.6: User Contact Information.

# User Permissions

User permissions can be accessed from the **Manage Users** webpage. **Select** a user from the list to view the User Management and Permissions webpage to edit permissions.

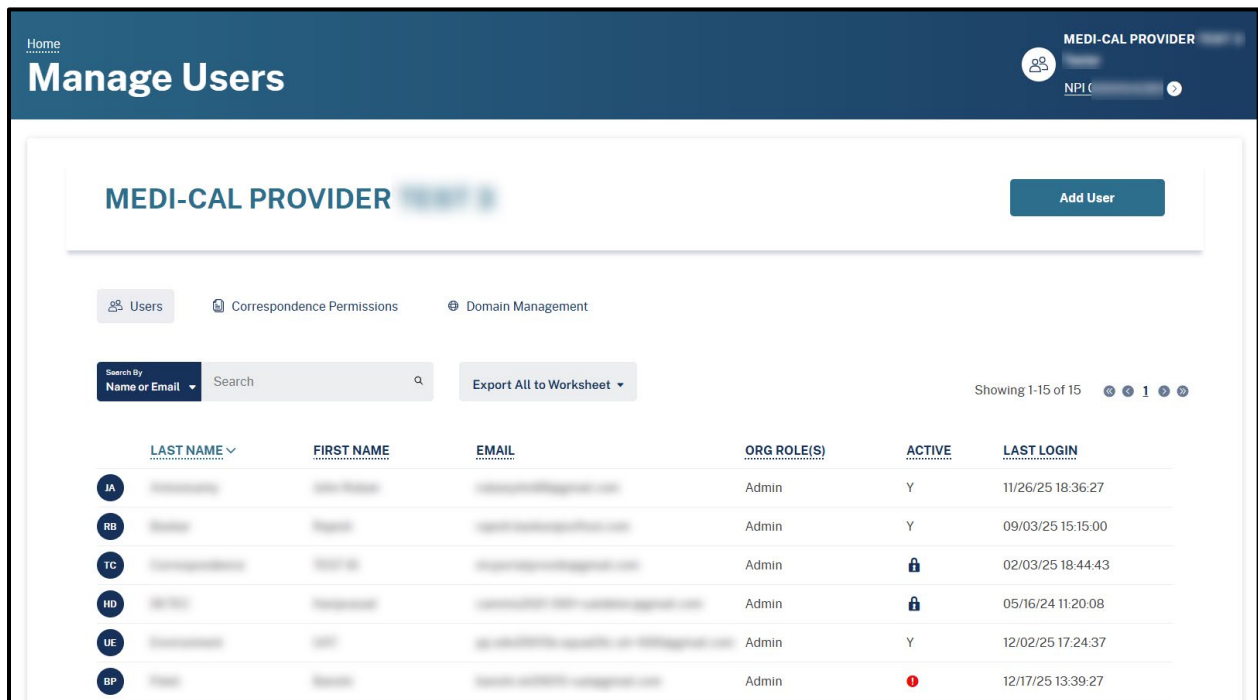
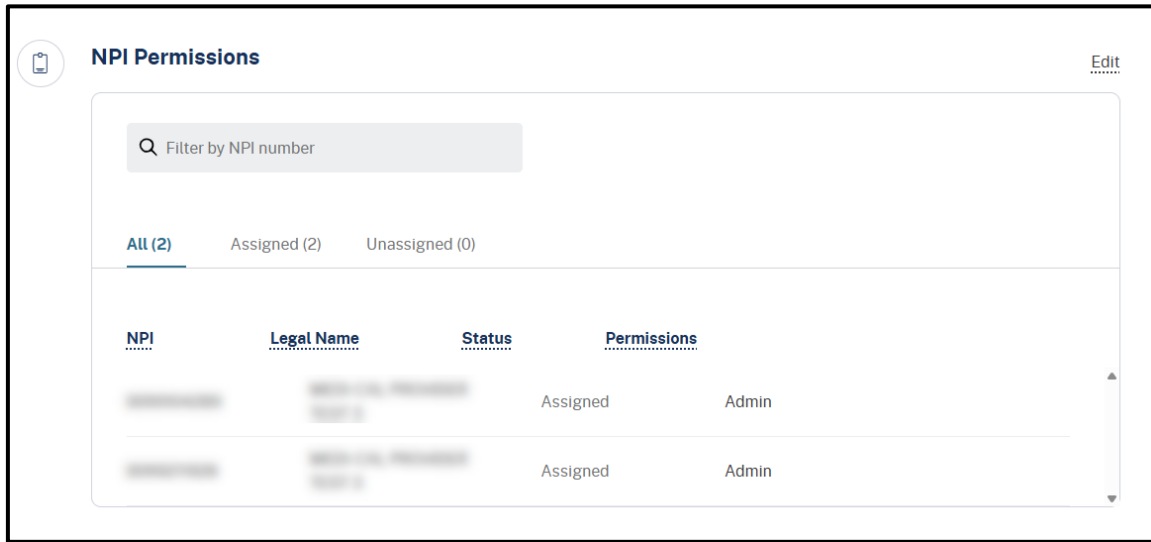


Figure 5.7: Manage Users Webpage.

# NPI Permissions

Administrators can assign users to NPIs within an organization and select permission levels. If the user is an Organization Administrator they will have automatically been given full permission to all NPIs. All NPIs do not have to be assigned.

An NPI can be located by entering it in the search field or use the tabs above the NPI list to narrow the list from All to Assigned or Unassigned. Select the Edit hyperlink to switch to edit mode



**Figure 5.8:** NPI Permissions Section.

1. Select one of the following levels of permission for each NPI:
  - **Administrator:** Users with an NPI role of administrator will have access to view and reset NPI PINs, view tax documents and correspondence that have been granted to them by their Organization Administrator. They will not have access to add, remove or modify users if they are not assigned the Organization Administrator role.
  - **Processor:** Users with an NPI role of processor will be able to view NPI PINs and correspondence that have been granted to them by their Organization Administrator. They will not be able to view tax documents.
  - **None:** User has no access to the NPI. This is the default setting.

2. Select the **Update** button to save the assigned permissions. These permissions can be changed at any time.

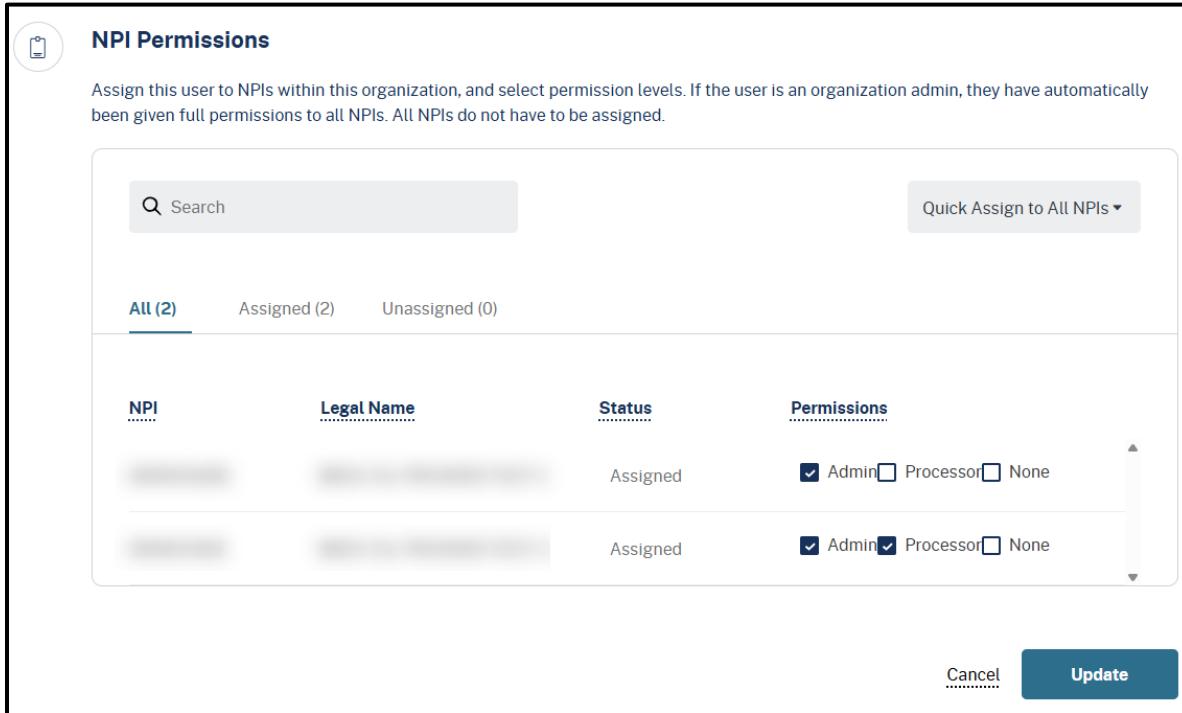


Figure 5.9: NPI Permissions Edit Mode.

## Quick Assign to All NPIs

1. The **Quick Assign to All NPIs** option assigns a user to all NPIs at a certain permission level. To select this feature, navigate to the dropdown menu and select the permissions level for the user.

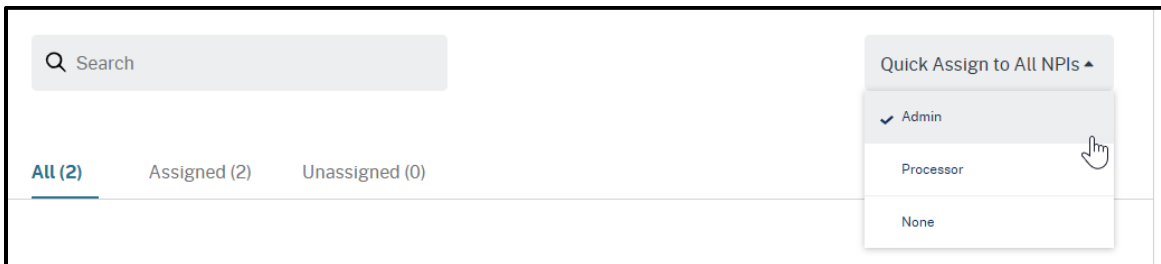


Figure 5.10: NPI Permissions Quick Assign Options.

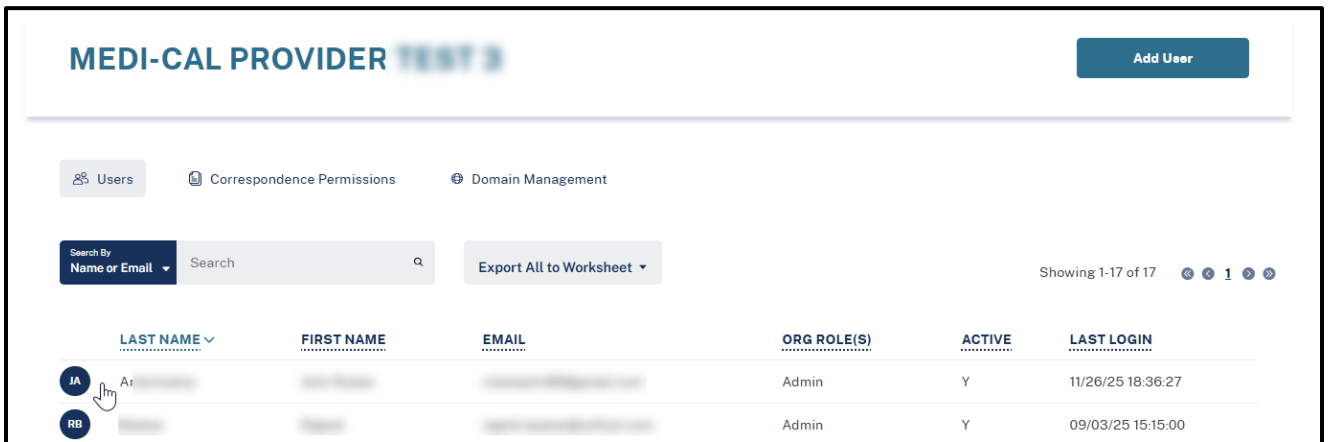
# Correspondence Permissions

## Assign Individual User Permissions

From the **User Management and Permissions** webpage Administrators can assign individual user permissions to view and download selected correspondence types. Users must be assigned to an NPI to have access to correspondence.

Use the search function to find a specific name, email or NPI. Alternatively, users can be viewed by name, email, role, activity or last login date from the list.

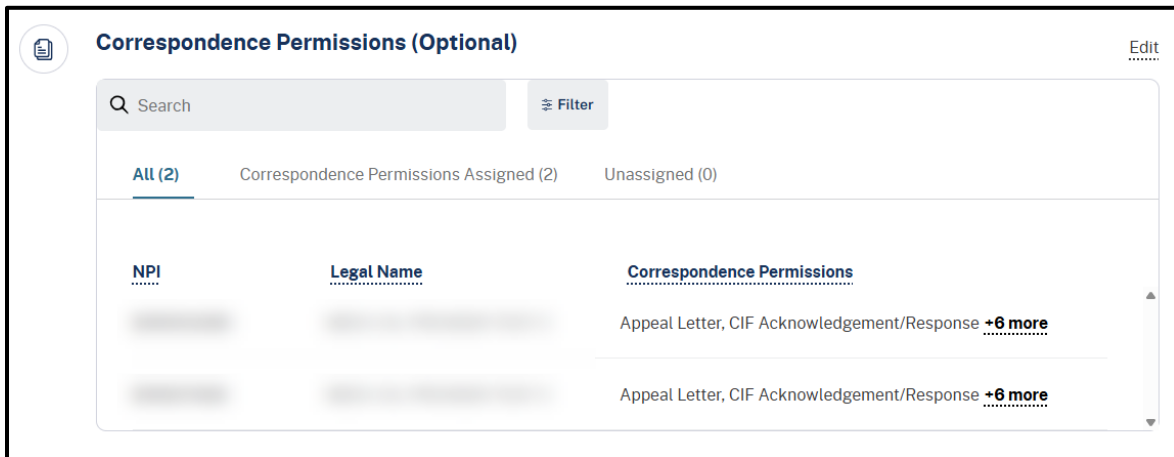
1. **Select** a name from the list on the **Manage Users** webpage.



**Figure 5.11:** Select an Individual User Account.

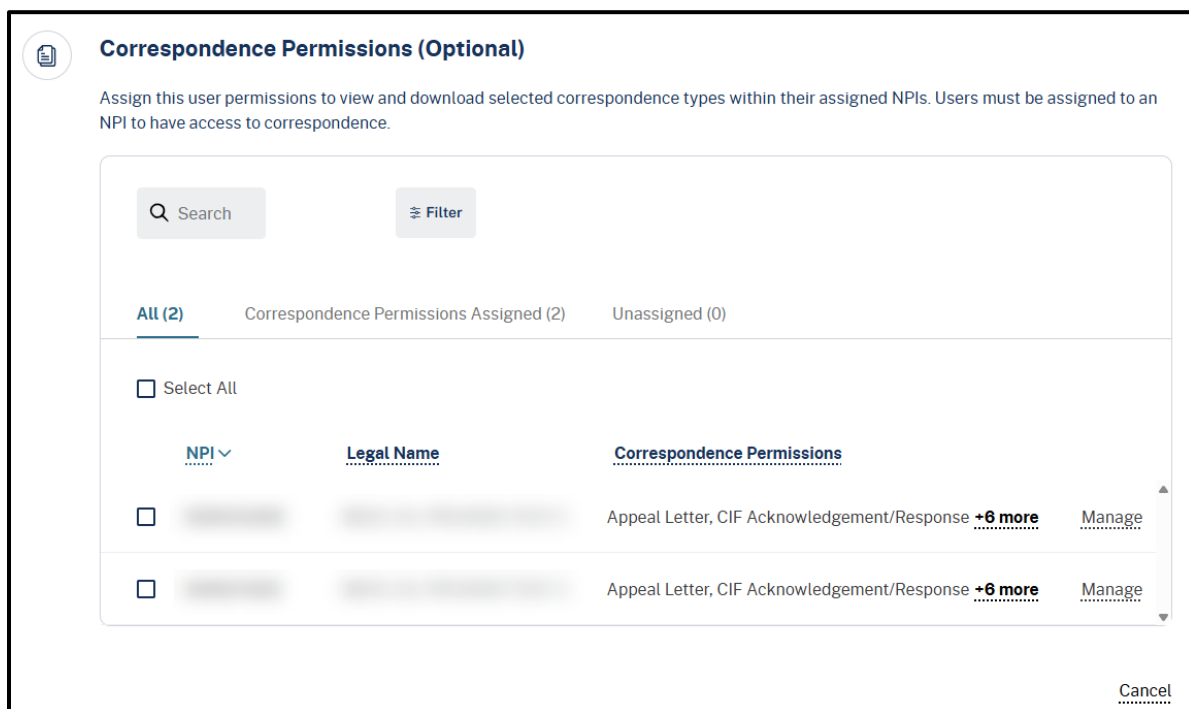
2. Scroll to the **Correspondence Permissions** section
  - Locate an NPI by entering it in the search field. Filter correspondence by one or more types by selecting the Filter dropdown. Use the tabs above the NPI list to narrow the list to **All**, **Correspondence Permissions Assigned** or **Unassigned**.
  - View the assigned list of correspondence types under the **Correspondence Permissions** column. The initial list of correspondence is limited to one row of items. Expand the list by selecting the **(+) more** hyperlink.

3. Select the **Edit** hyperlink to enter edit mode and manage permissions.



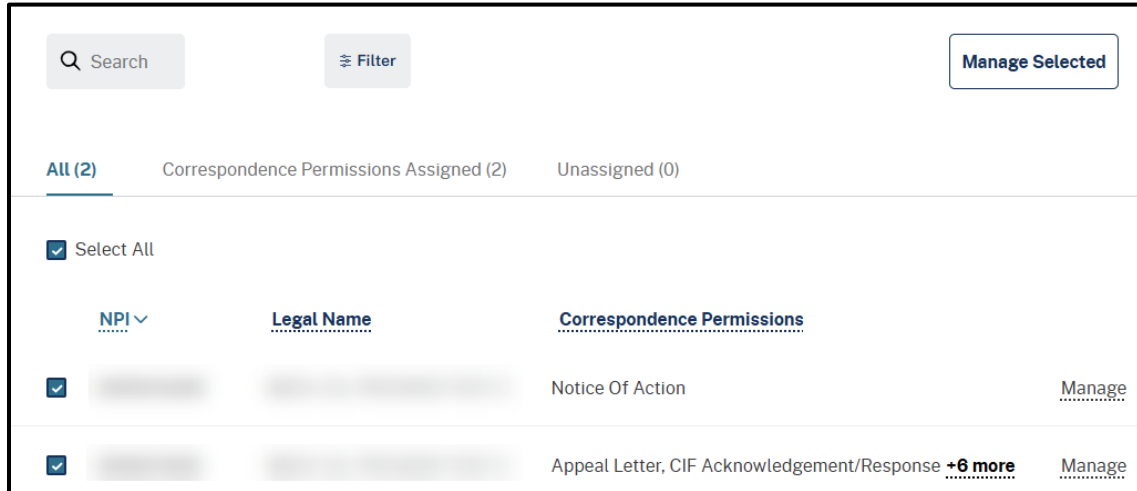
**Figure 5.12:** Correspondence Permissions Section.

4. Select the **Manage** hyperlink to view the complete list of available correspondence types.



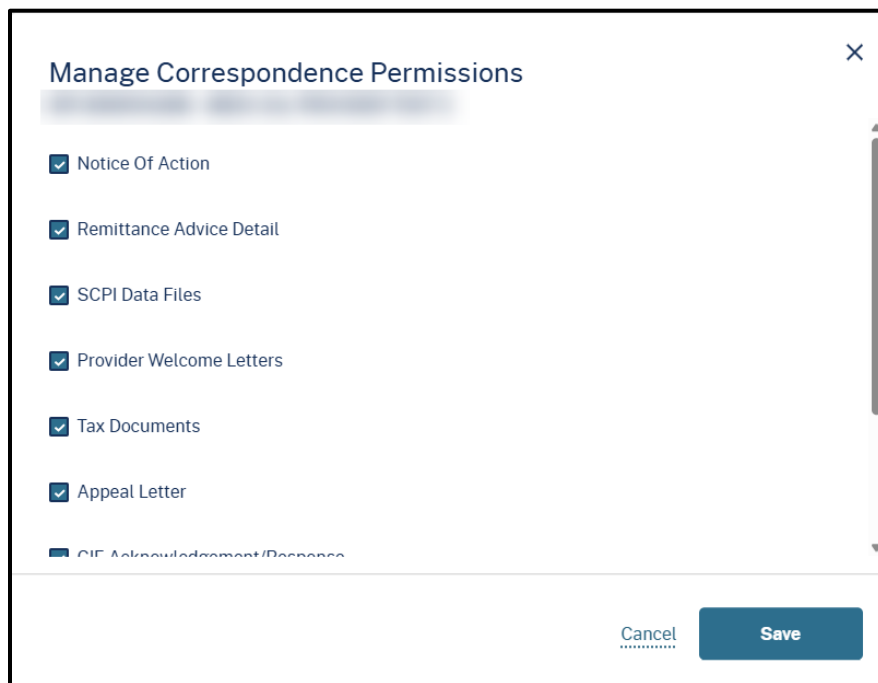
**Figure 5.13:** Correspondence Permissions Edit Mode.

5. Manage multiple NPIs in the list concurrently by selecting the **Select All** checkbox then the **Manage Selected** button.



**Figure 5.14:** Manage Multiple NPIs.

6. Check the box(es) of the types of correspondence this user can access. Select the **Save** button to confirm correspondence options.



**Figure 5.15:** Manage Correspondence Permissions Pop-Up.

7. When all permissions are set, select **Cancel** to exit.

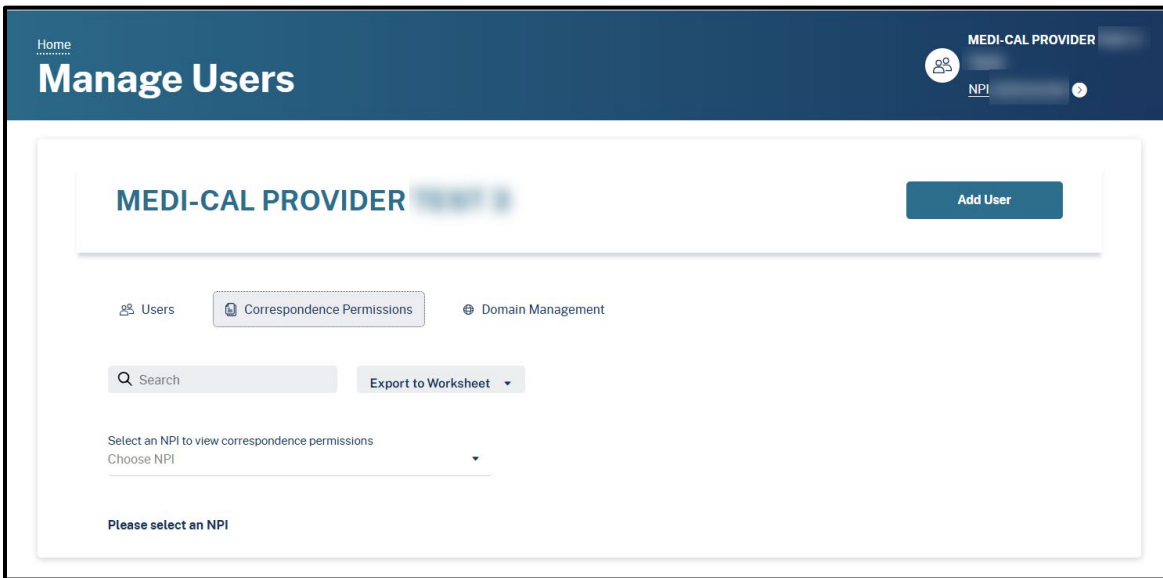


**Figure 5.16:** Exit Correspondence Permissions Edit Mode.

## NPI Level Correspondence Permissions

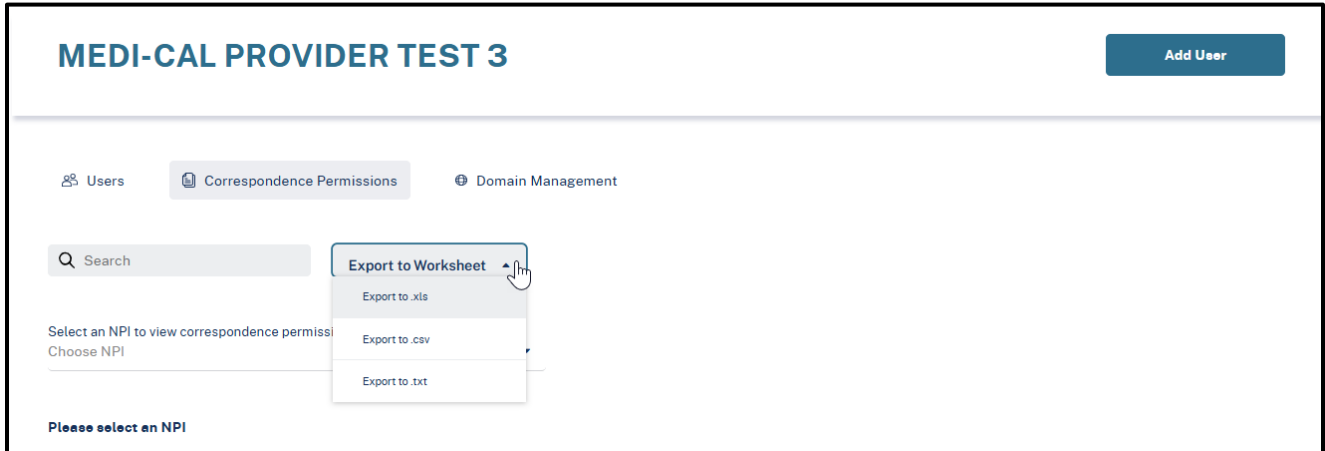
An Organization Administrator can view NPI-level correspondence permissions by correspondence type or the users assigned to that correspondence and edit the user's information. This is a different administrative perspective from the correspondence permissions at the level when adding a user

1. Select the **Correspondence Permissions** tab on the Manage Users webpage.



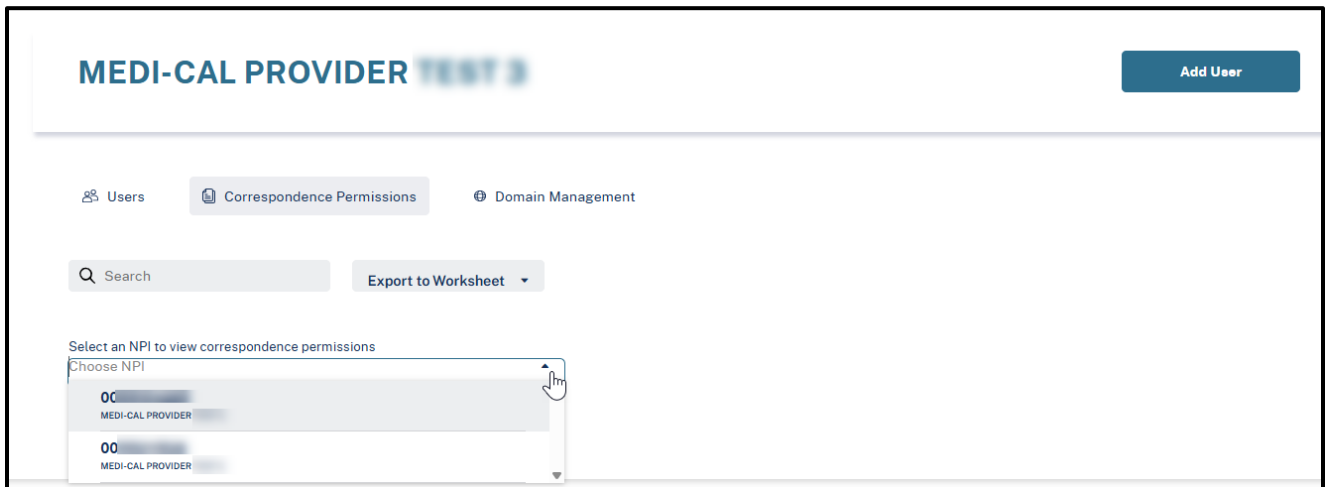
**Figure 5.17:** Correspondence Permissions Tab.

2. Search for specific NPI to view correspondence permissions and export the data to a worksheet.



**Figure 5.18:** Export Function.

3. Select an NPI from the **drop-down menu**.



**Figure 5.19:** NPI Selection Drop-Down Menu.

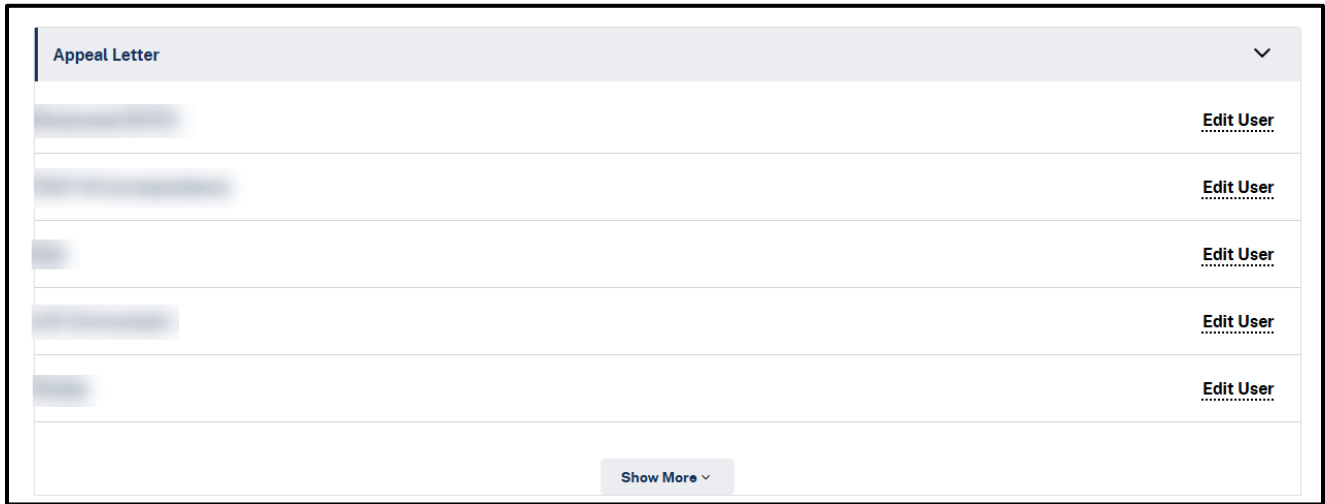
4. A list of all correspondence types appears. Select the **type of correspondence** to expand the list item and view the users associated with the permission type.

The screenshot displays a web application interface for 'MEDI-CAL PROVIDER'. At the top right, there is a blue 'Add User' button. Below the header, there are three navigation tabs: 'Users', 'Correspondence Permissions' (which is active), and 'Domain Management'. A search bar and an 'Export to Worksheet' button are located below the tabs. A dropdown menu is set to 'Select an NPI to view correspondence permissions' with the selected option being '- MEDI-CAL PROVIDER'. The main content area is a list of correspondence types, each in a light gray box with an upward-pointing arrow on the right side:

- Appeal Letter
- CIF Acknowledgement/Response
- Notice of Action
- Provider Check Acknowledgement
- Remittance Advice Detail
- SCPI Data Files
- Tax Documents
- Provider Welcome Letters

**Figure 5.20:** NPI Correspondence Types.

5. Select the **Edit User** hyperlink to proceed to the next step.



**Figure 5.21:** Expanded Correspondence Type.

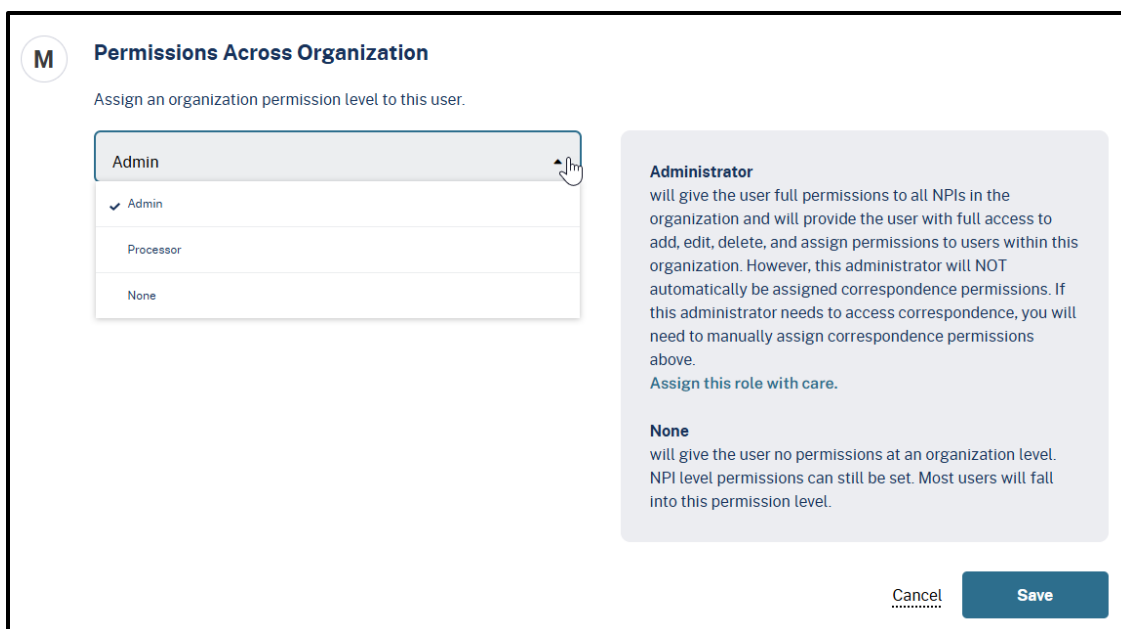
## Permissions Across Organization

1. Select the **Edit** hyperlink.



**Figure 5.22:** Permissions Across Organization Section.

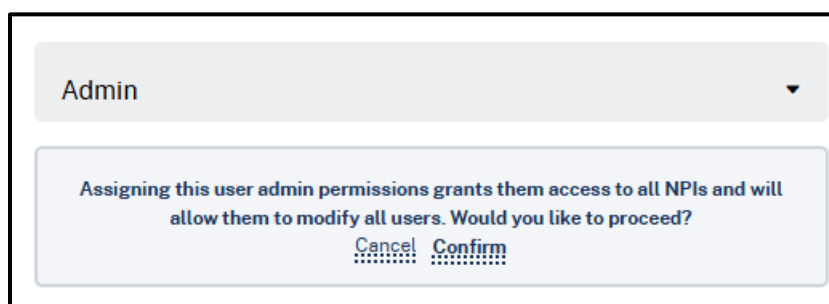
2. Select a permission level from the dropdown menu. Select **Save**.



**Figure 5.23:** Permissions Across Organization Edit Mode.

**Note:** Read and understand the descriptions of the levels of permission for each role. The Admin role will give the user full permissions to all NPIs in the organization and will provide the user with full access to add, edit, delete, and assign permissions to users within this organization.

3. A confirmation message appears if a role is changed from either Processor or None to Admin. Select **Confirm** if this is the correct permission level or **Cancel** to return to its previous level.



**Figure 5.24:** Admin Confirmation.

# Reactivate User

Complete the following to deactivate or reactivate a user:

1. To find the appropriate user, use the **search bar** and search for the desired user or select a user from the list. An inactive user can be identified by a **(N)** icon in the Active column.

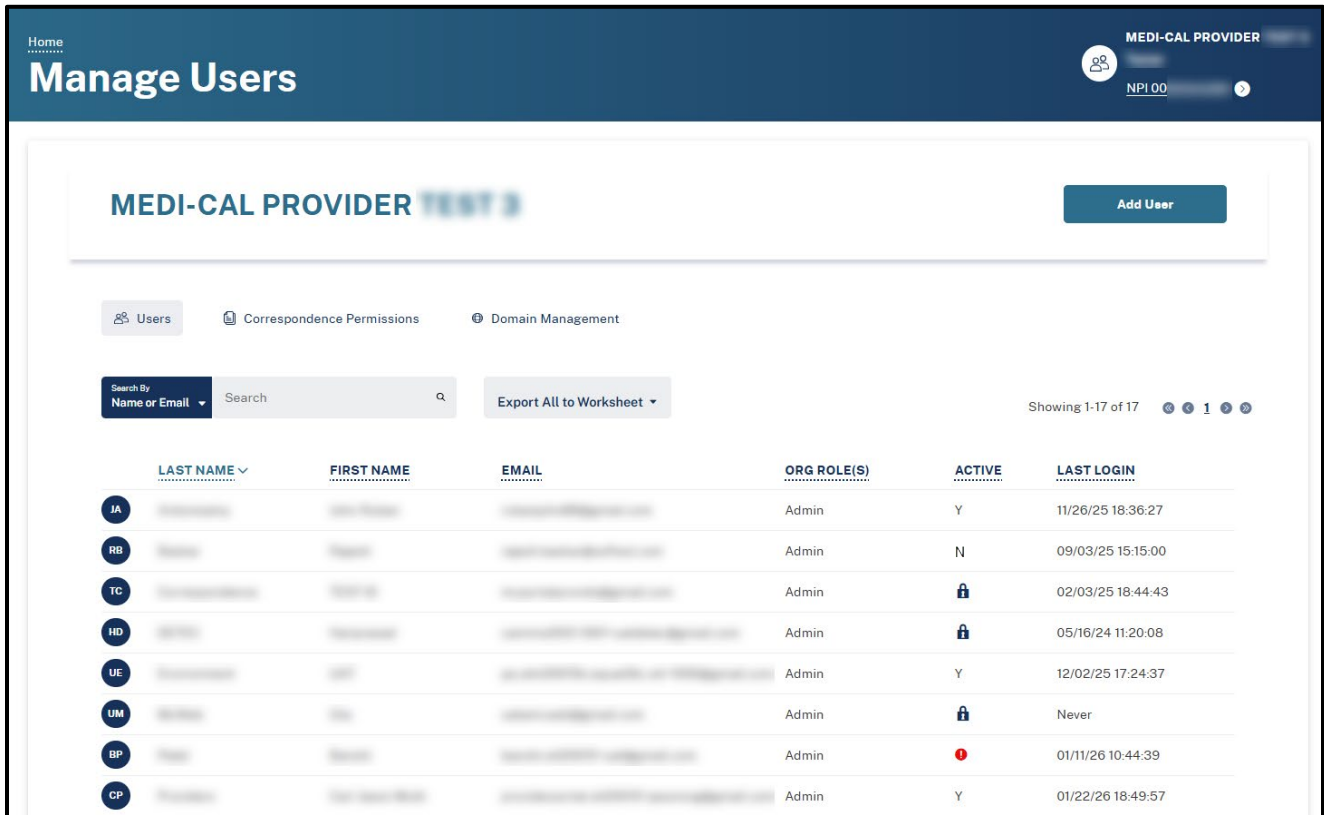


Figure 5.25: Manage Users Page.

2. The user's account information appears. Select the kebab menu icon (⋮) at the right corner and select **Reactivate user**.

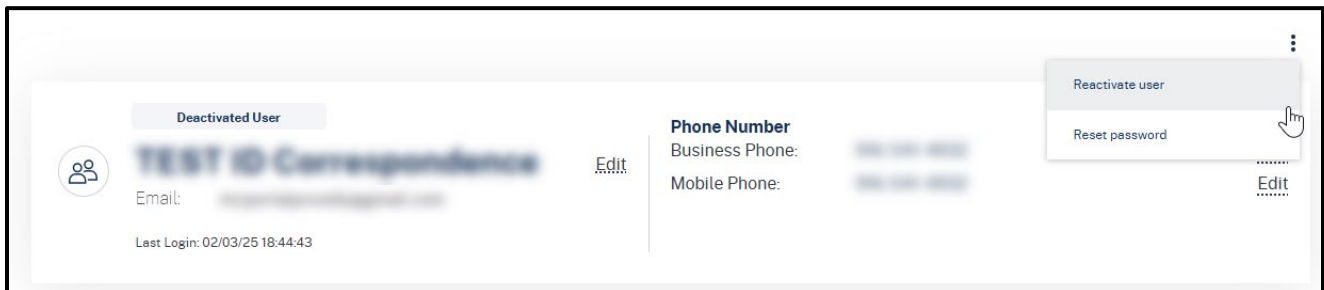


Figure 5.26: Reactivate User Option.

3. A pop-up window appears prompting to reactivate this user. Select **Confirm**.

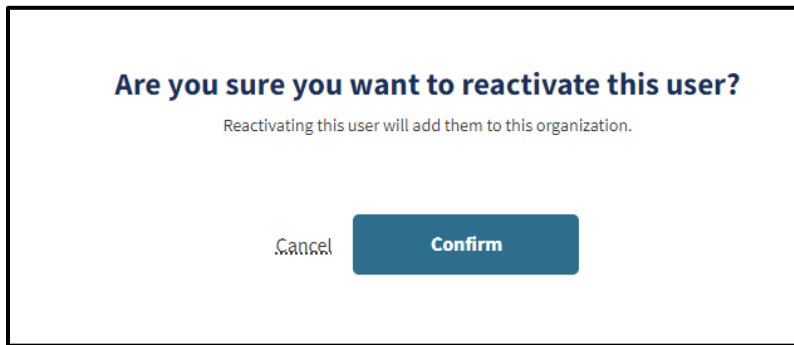


Figure 5.27: Reactivate User Confirmation.

## Deactivate User

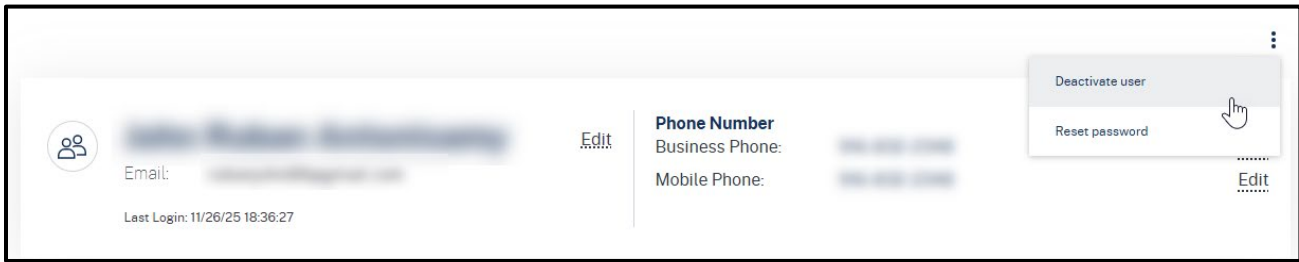
An active user, locked user or user with an expired registration link can be deactivated.

1. To find the appropriate user, use the **search bar** and search for the desired user or select a user from the list. An active user can be identified by a **(Y) icon** in the Active column.

	LAST NAME	FIRST NAME	EMAIL	ORG ROLE(S)	ACTIVE	LAST LOGIN
JA				Admin	Y	11/26/25 18:36:27
RB				Admin	Y	09/03/25 15:15:00
TC				Admin	🔒	02/03/25 18:44:43
HD				Admin	🔒	05/16/24 11:20:08
UE				Admin	Y	12/02/25 17:24:37
BP				Admin	🚫	12/17/25 13:39:27

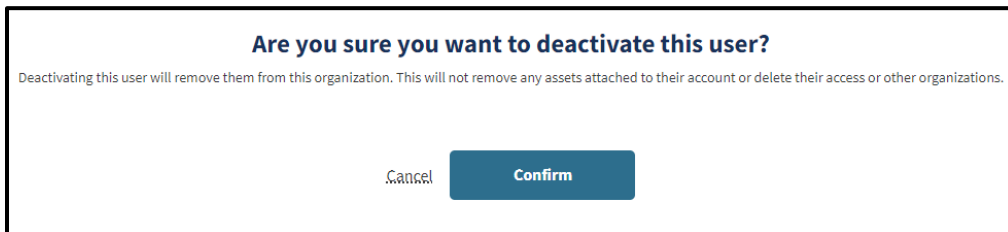
Figure 5.28: Manage Users Page.

- The user's account information appears. Select the kebab menu icon ( ⋮ ) at the right corner and select **Deactivate user**.



**Figure 5.29:** Deactivate User Option.

- A pop-up window appears prompting to deactivate this user. Select **Confirm**.



**Figure 5.30:** Confirmation to Deactivate User.

## Unlock An Account

A user account will become locked if it is inactive in the Provider Portal for more than 180 days. Users should log in at least once a month to prevent their account from being locked. To unlock and reactivate the account, contact the organization administrator or Telephone Service Center. Passwords will remain locked until the password reset email is received and the password is updated.

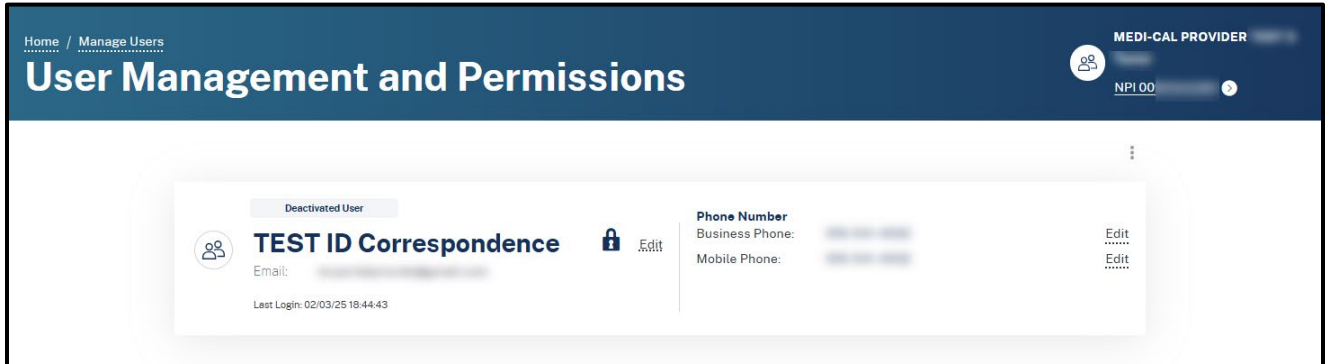
- Within the **Manage Users** webpage the accounts that are locked have the lock symbol ( 🔒 ) in the Active column.

 A screenshot of the 'MEDI-CAL PROVIDER' user management interface. At the top, there is a header with the title 'MEDI-CAL PROVIDER' and an 'Add User' button. Below the header are three tabs: 'Users', 'Correspondence Permissions', and 'Domain Management'. The 'Users' tab is selected. There is a search bar with 'Search by Name or Email' and an 'Export All to Worksheet' button. The main content is a table with the following columns: 'LAST NAME', 'FIRST NAME', 'EMAIL', 'ORG ROLE(S)', 'ACTIVE', and 'LAST LOGIN'. The table contains four rows of user data. The third and fourth rows have a lock icon in the 'ACTIVE' column, indicating they are locked.
 


LAST NAME	FIRST NAME	EMAIL	ORG ROLE(S)	ACTIVE	LAST LOGIN
JA			Admin	Y	11/26/25 18:36:27
RB			Admin	Y	09/03/25 15:15:00
TC			Admin	🔒	02/03/25 18:44:43
HD			Admin	🔒	05/16/24 11:20:08

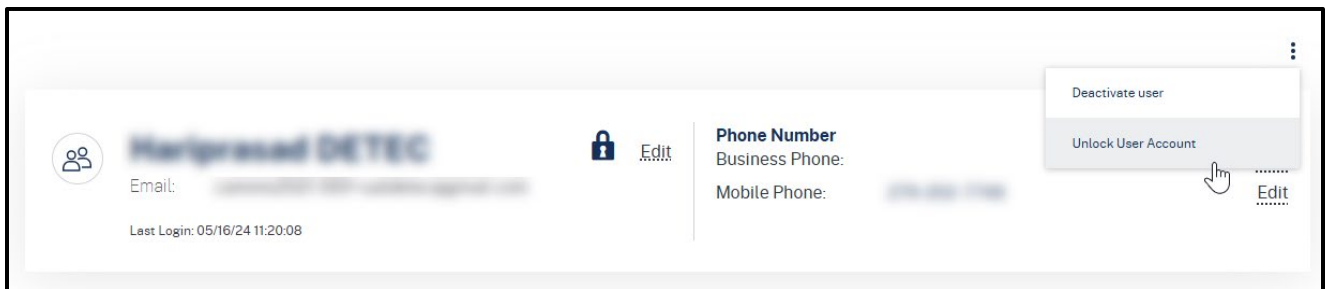
**Figure 5.31:** User Management Table.

2. Select the user account to unlock the account. A **Deactivated User** label appears above the user's name.



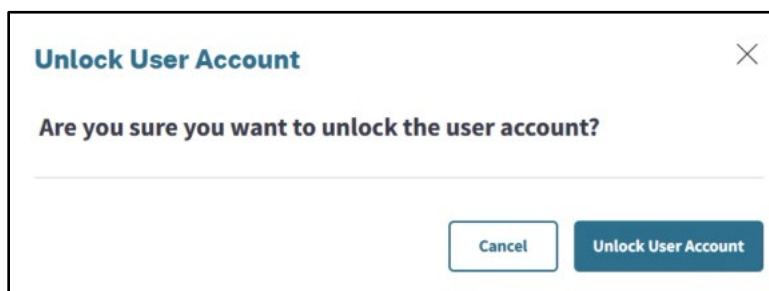
**Figure 5.32:** User Account Details.

3. Select the **kebab menu** icon (  ) at the right corner and select **Unlock User Account**.



**Figure 5.33:** Unlock User Account Menu Option.

3. A pop-up screen will appear. Select **Unlock User Account** to proceed.




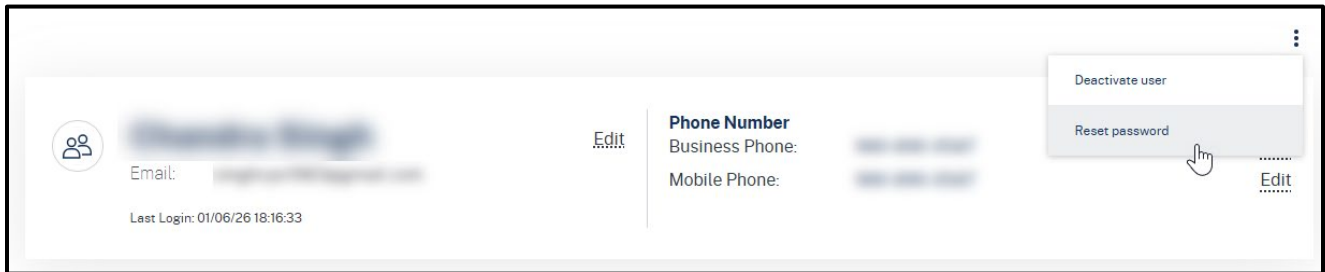
**Figure 5.34:** Unlock User Account Message.

4. Once complete, the account will successfully be unlocked, and the user will receive an email to reset their password.

# Reset Password

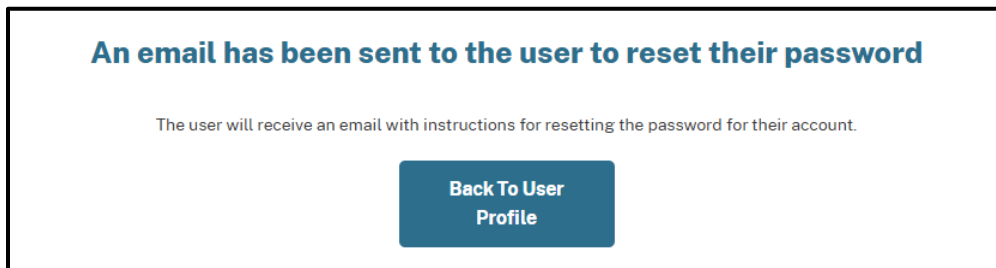
Organization Administrators can reset passwords for active users, inactive users or users whose registration link has expired.

1. Within the **Manage Users** webpage, select the user account that needs a password reset.
2. Select the **kebab menu** icon (  ) at the right corner, then choose **Reset password**.



**Figure 5.35:** Reset Password Option.

3. A confirmation screen appears indicating that an email has been sent to the user for them to reset their password. Select **Back To User Profile** to conduct additional actions on this user account.

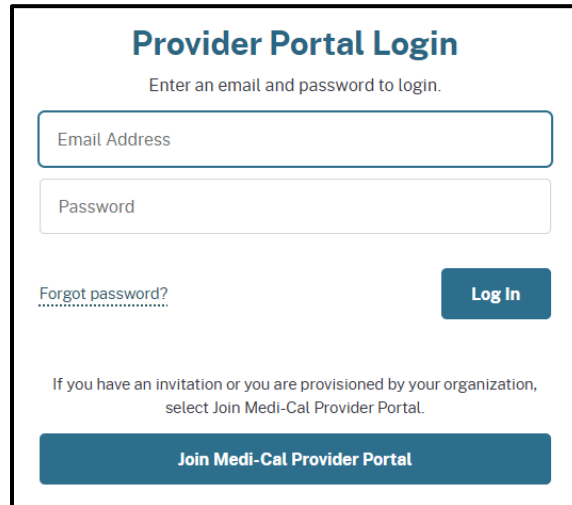


**Figure 5.36:** Email Reset Message.

# Forgotten Password at Login

If the user forgets their password they can reset it by doing the following:

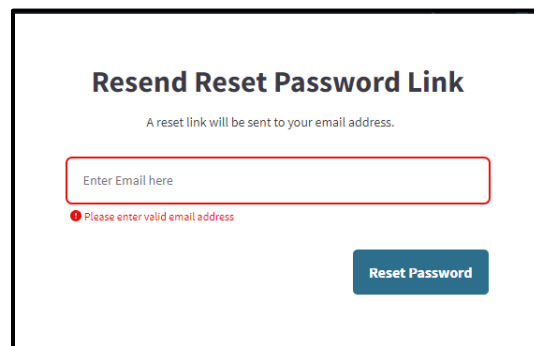
1. From the Log In screen, select **Forgot password?**



The screenshot shows the 'Provider Portal Login' interface. At the top, it says 'Provider Portal Login' in blue, followed by the instruction 'Enter an email and password to login.' Below this are two input fields: 'Email Address' and 'Password'. To the left of the 'Log In' button is a link for 'Forgot password?'. The 'Log In' button is a dark blue rectangle with white text. Below the input fields, there is a note: 'If you have an invitation or you are provisioned by your organization, select Join Medi-Cal Provider Portal.' At the bottom, there is a large dark blue button labeled 'Join Medi-Cal Provider Portal'.

**Figure 5.37:** Provider Portal Login.

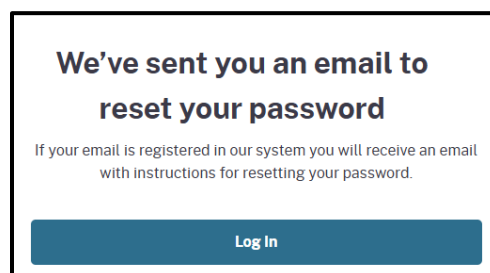
2. A **Resend Reset Password Link** screen will appear. Enter the appropriate email address and select **Reset Password**.



The screenshot shows the 'Resend Reset Password Link' screen. The title is 'Resend Reset Password Link' in bold. Below it, it says 'A reset link will be sent to your email address.' There is a text input field with the placeholder 'Enter Email here'. Below the input field, there is a red error message: 'Please enter valid email address'. To the right of the input field is a dark blue button labeled 'Reset Password'.

**Figure 5.38:** Resend Reset Password Link.

3. A notification will appear stating an email has been sent to reset password.

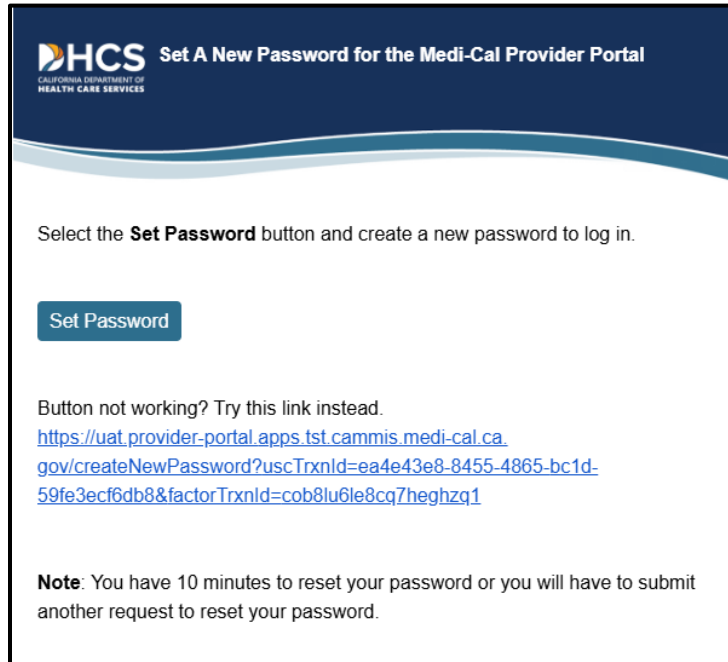


The screenshot shows a notification screen with the heading 'We've sent you an email to reset your password' in bold. Below the heading, it says 'If your email is registered in our system you will receive an email with instructions for resetting your password.' At the bottom, there is a dark blue button labeled 'Log In'.

**Figure 5.39:** Notification of Email Sent to Reset Password.

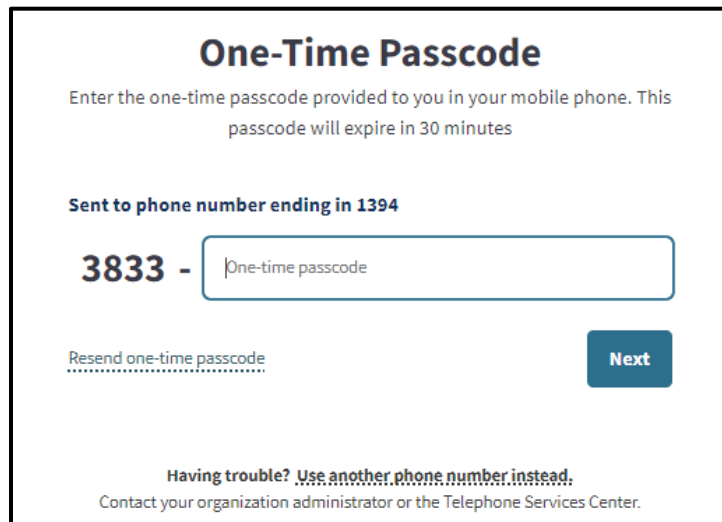
4. A link to reset the password will be sent via email. Select **Set Password**.

**Note:** Password reset is limited to 10 minutes for security reasons.



**Figure 5.40:** Set New Password Email Notification.

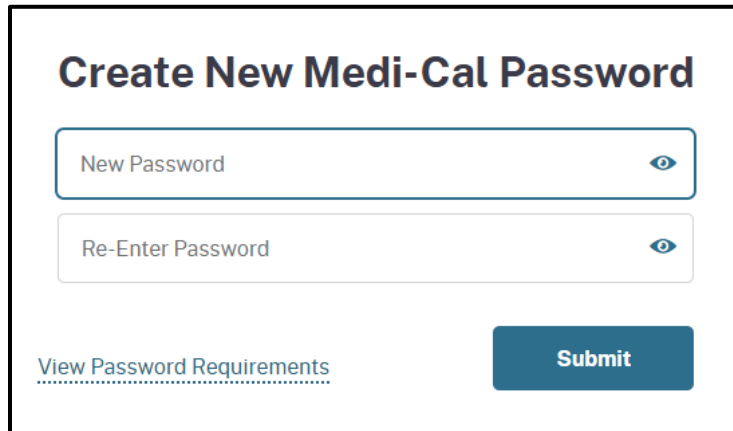
5. Check the mobile device for the OTP and enter secure code into the field. Select **Next**.



**Figure 5.41:** Enter the OTP.

6. The **Create New Medi-Cal Password** page displays and the user can enter a new password and select **Submit**. A confirmation screen appears, and the password is updated.

Note: The password must be a minimum of 15 characters and contain at least one uppercase letter, one lowercase letter, one numeral and one special character. A recently used password cannot be reused.



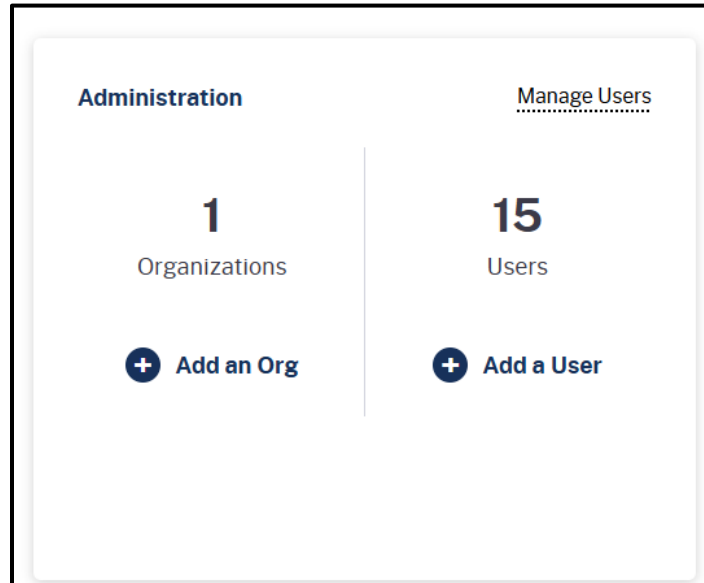
The screenshot shows a web form titled "Create New Medi-Cal Password". It features two input fields: "New Password" and "Re-Enter Password", each with a toggle icon (an eye) to the right. Below the fields is a link labeled "View Password Requirements" and a blue "Submit" button.

**Figure 5.42:** Create New Medi-Cal Password.

# Domain Management

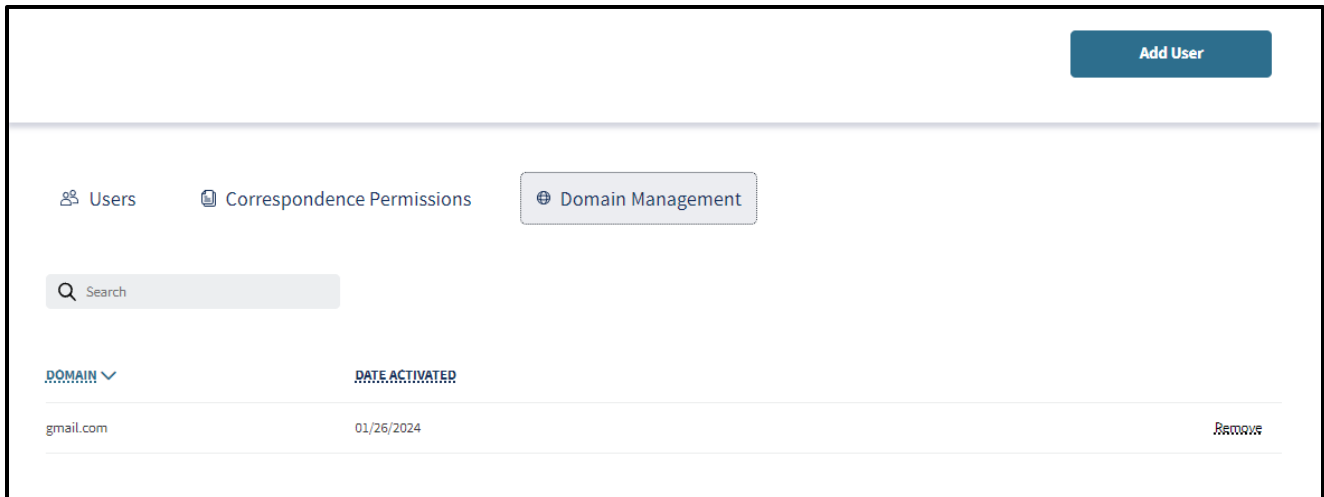
To remove an unwanted domain from an organization ensure that there are no active users with that email address. If there are, those users must be deactivated first to remove the domain. This area may only be accessed by individuals who are designated as Organization Administrators.

1. In the Administration tile, select **Manage Users**.



**Figure 5.43:** Administration Tile.

2. Select **Domain Management**.
3. Select **Remove** next to the domain that should be removed.

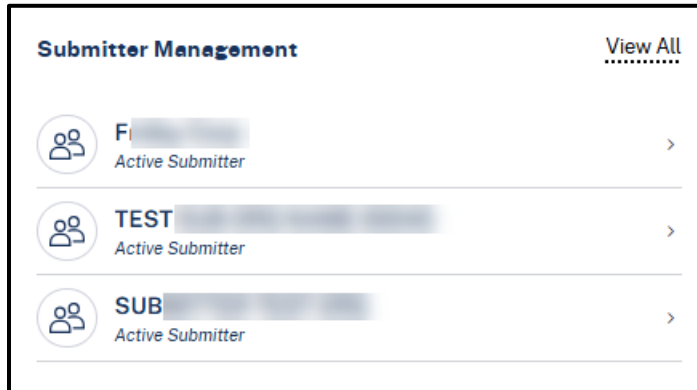


**Figure 5.44:** Domain Management.

# Submitter Management

Individuals designated by Organizational Administrators can submit or approve new affiliations with registered submitter organizations.

1. From the Dashboard select **View All** from the Submitter Management tile.

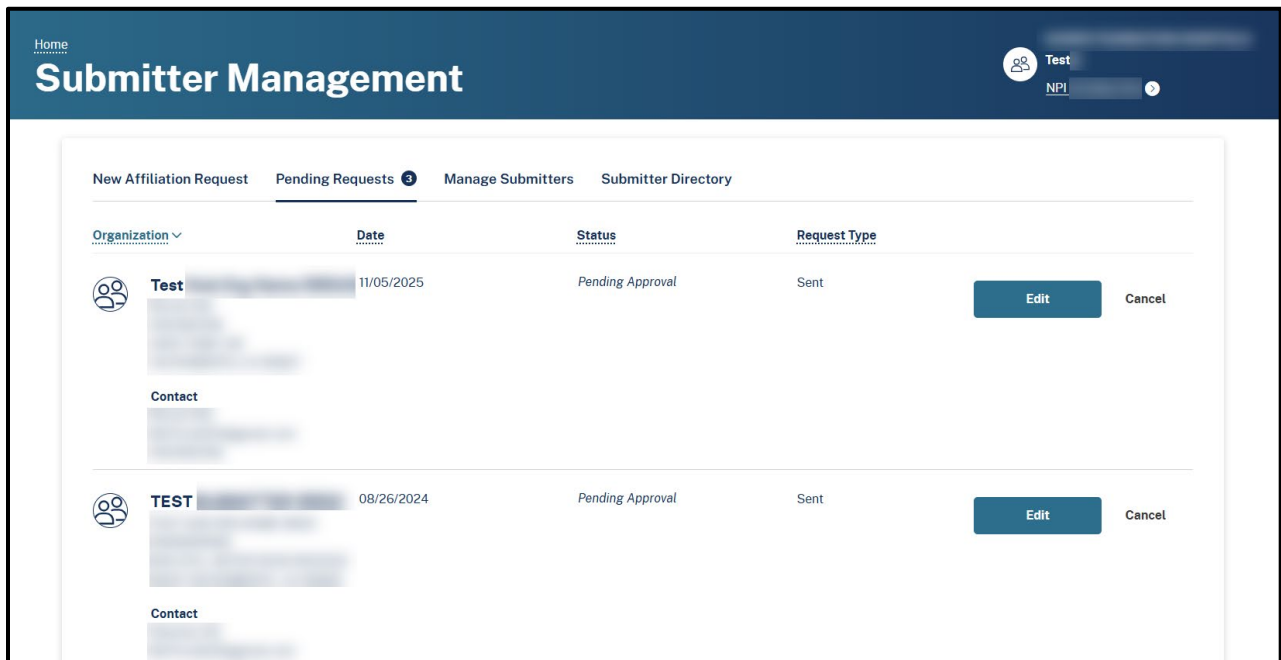


**Figure 6.1:** Submitter Management.

Users assigned as NPI Admins will have limited access within the **Submitter Management** page and will not be able to submit, approve or deny affiliation requests.

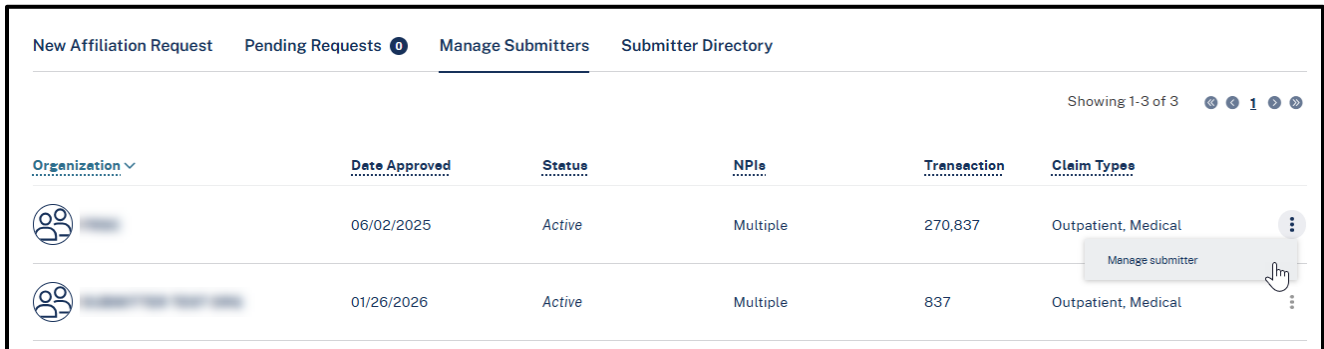
The Pending Requests tab on the **Submitter Management** webpage will open.





2. Select **Edit** to change the current organization permissions.



**Figure 6.2:** Pending Requests.

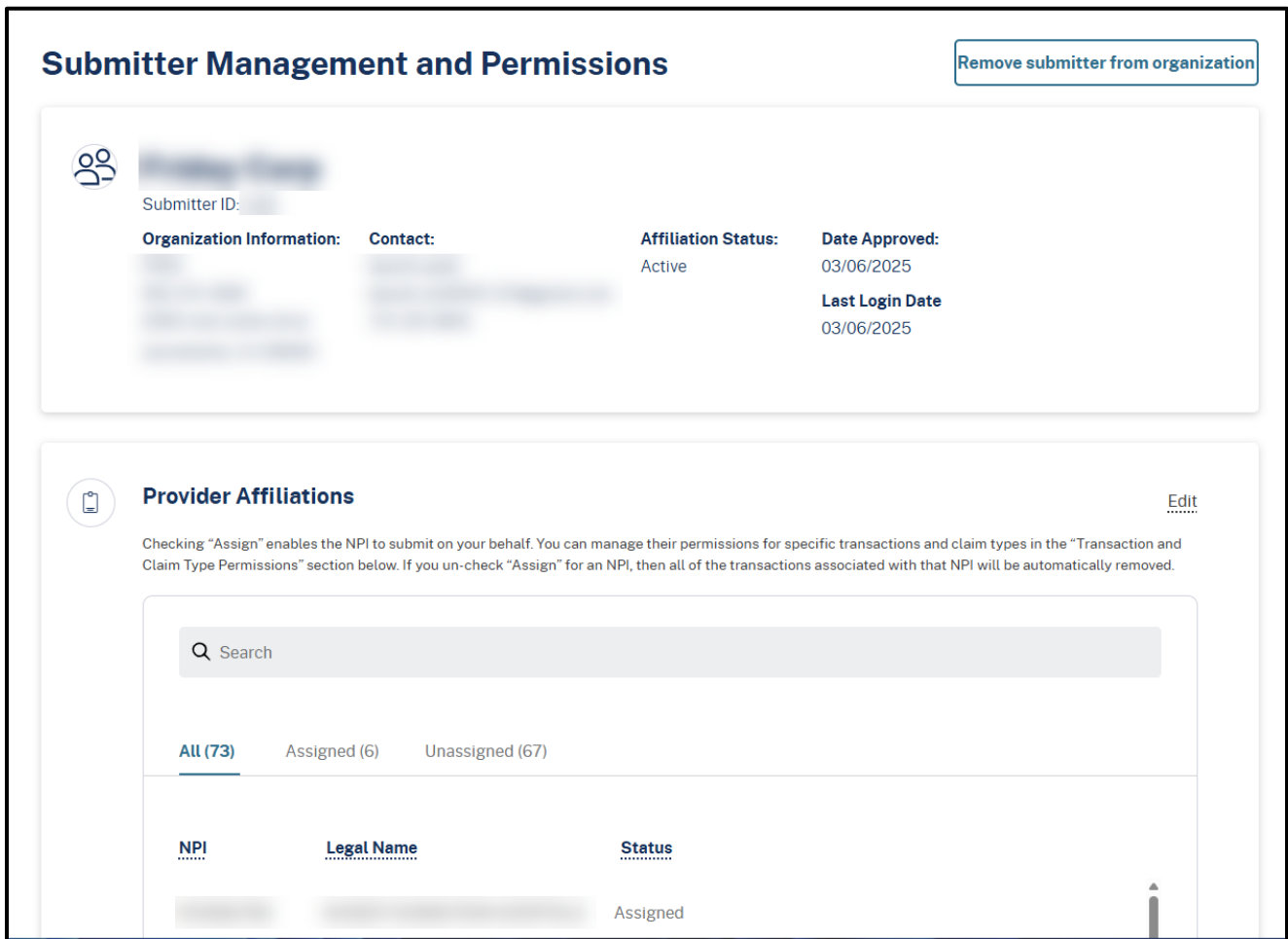
3. Select the **kebab menu** icon (  ) then **Manage submitter**.



Organization	Date Approved	Status	NPIs	Transaction	Claim Types	
	06/02/2025	Active	Multiple	270,837	Outpatient, Medical	 Manage submitter
	01/26/2026	Active	Multiple	837	Outpatient, Medical	


**Figure 6.3:** Manage Submitters.

The **Submitter Management and Permissions** page reveals all management options including the ability to remove the submitter from the organization, edit provider affiliations, transaction and claim type permissions and view the Submitter + Provider Affiliation Agreement.



### Submitter Management and Permissions

[Remove submitter from organization](#)

 **Submitter ID:** [Redacted]

**Organization Information:** [Redacted]    **Contact:** [Redacted]    **Affiliation Status:** Active    **Date Approved:** 03/06/2025

[Redacted]    [Redacted]    **Last Login Date:** 03/06/2025

#### Provider Affiliations Edit

Checking "Assign" enables the NPI to submit on your behalf. You can manage their permissions for specific transactions and claim types in the "Transaction and Claim Type Permissions" section below. If you un-check "Assign" for an NPI, then all of the transactions associated with that NPI will be automatically removed.

Q Search

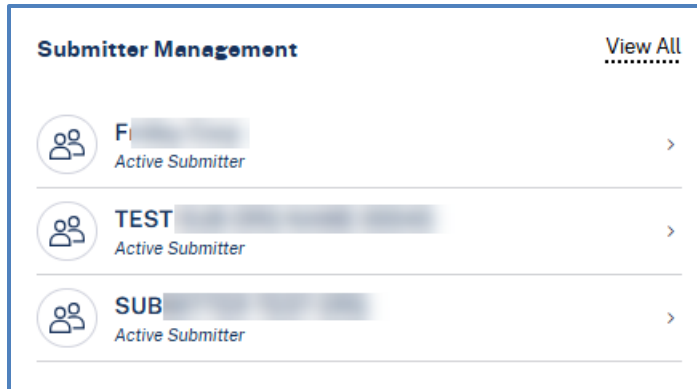
[All \(73\)](#)    Assigned (6)    Unassigned (67)

NPI	Legal Name	Status
[Redacted]	[Redacted]	Assigned

**Figure 6.4:** Submitter Management and Permissions Page.

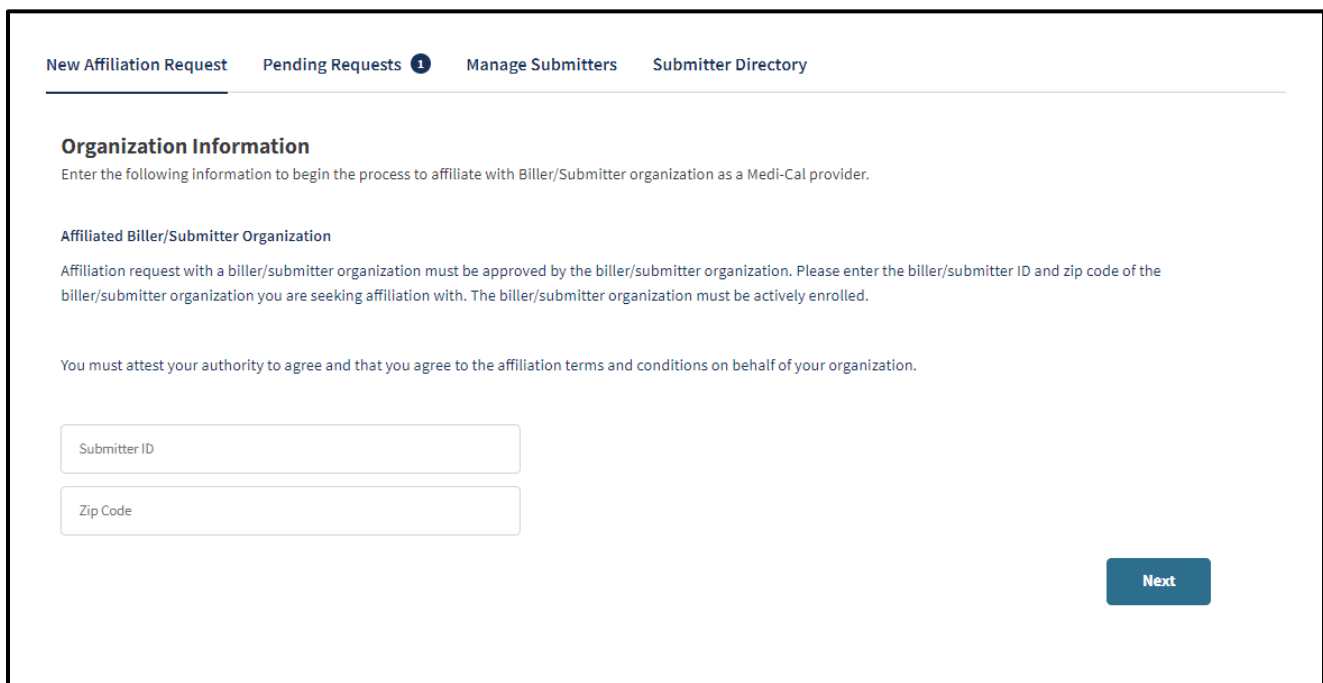
# New Affiliation Request to a Submitter Organization

1. Select **View All** from the Submitter Management tile in the Dashboard.



**Figure 6.5:** Submitter Management Tile on Dashboard.

2. Under the **New Affiliation Request** tab, enter the **Organization Information (Submitter ID and Zip Code)** of the submitter organization. Select **Next**.



**Figure 6.6:** New Affiliation Request.

**Note:** The submitter organization must be actively enrolled in the Provider Portal to request affiliation. The new request is valid for 60 days until the Submitter Organization approves the affiliation. If approval isn't received, the affiliation request can be resubmitted.

- Complete the *Medi-Cal Telecommunications Provider and Biller Application/Agreement* (DHCS 6153). Read the agreement form and then sign with First and Last name along with Title. Select **Next**.

**Medi-Cal Telecommunications Provider and Biller Application/Agreement**

DHCS and the California MMIS Fiscal Intermediary require a signed telecommunication application/agreement form from CMC submitters.

Submitter + Provider Affiliation Agreement  TEST SUB ORG NAME 00045  Not signed

submission, shall mean any claim submitted through any electronic means such as: modem communications.

**3.0 CLAIMS ACCEPTANCE AND PROCESSING**  
The Department agrees to accept from the enrolled Provider/Biller, electronic claims submitted to the Medi-Cal fiscal intermediary in accordance with the Medi-Cal provider manuals. The Provider hereby acknowledges that he has received, read, and understands the provider manual and its contents, and agrees to read and comply with all provider manual updates and provider bulletins relating to electronic billing.

**3.1 CLAIMS CERTIFICATION**  
The Provider agrees and shall certify under penalty of perjury that all claims for services submitted electronically have been personally provided to the patient by the Provider or under his direction by another person eligible under the Medi-Cal Program to provide to such services, and such person(s) are designated on the claim. The services were, to the best of the Provider's knowledge, medically indicated and necessary to the health of the patient. The Provider shall also certify that all information submitted electronically is accurate and complete. The Provider understands that payment of these claims will be from federal and/or state funds, and that any falsification or concealment of a material fact may be prosecuted under federal and/or state laws. The Provider/Biller agrees to keep for a minimum period of three years from the date of service an electronic archive of all records necessary to fully disclose the extent of services furnished to the patient. A printed representation of those records shall be produced upon request of the Department during that period of time. The Provider/Biller agrees to furnish these records and any information regarding payments claimed for providing the services, on request, within the State of California to the California Department of HealthCare Services; California Department of Justice; Office of the State Controller; U.S. Department of Health and Human Services; or their duly authorized representatives. The Provider also agrees that medical care services are offered and provided without discrimination based on race, religion, color, national or ethnic origin, sex, age, or physical or mental disability. The Provider/Biller agrees that using his Medi-Cal Submitter ID plus DHCS-issued password when submitting an electronic claim will identify the submitter and shall serve as acceptance to the terms and conditions of the Department's Telecommunications Provider and Biller Application/Agreement (DHCS 6153), paragraph 3.0. The Provider/Biller further acknowledges the necessity of maintaining the privacy of the DHCS-issued password and agrees to bear full responsibility for use or misuse of the Medi-Cal Submitter ID and password should privacy not be maintained.

**3.2 VERIFICATION OF CLAIMS WITH SOURCE DOCUMENTS**  
Regardless of whether the Provider employs a Biller, the Provider agrees to retain personal responsibility for the development, transcription, data entry, and transmittal of all claim information for payment. This includes usual and customary charges for services rendered. The Provider shall also assume personal responsibility for verification of submitted claims with source documents. The Provider/Biller agrees that no claim shall be submitted until the required source documentation is completed and made readily retrievable in accordance with Medi-Cal statutes and regulations. Failure to make, maintain, or produce source documents shall be cause for immediate suspension of electronic billing privileges.

**3.3 ACCURACY AND CORRECTION OF CLAIMS OR PAYMENTS**  
The Provider agrees to be responsible for the review and verification of the accuracy of claims payment information promptly upon the receipt of any payment. The Provider agrees to seek correction of any claim errors through the appropriate processes as designated by the Department or its fiscal intermediary including, but not limited to, the

I confirm that I am eligible to sign this agreement on behalf of my organization

First and Last Name  Title

I, the undersigned, am authorized and do attest and agree to all of the terms and conditions of this agreement.  
Electronic Signature: \_\_\_\_\_

**Figure 6.7:** Medi-Cal Telecommunications Provider and Biller Application/Agreement.

- A request complete screen will appear.

**Request Complete**

Your affiliation request has been sent to your selected submitter organization(s). Your request will be reviewed and you will be notified when your request is approved or denied.

[Back to Pending Requests](#)

**Figure 6.8:** Request Complete.

5. Once the submitter organization has signed the DHCS 6153, the Administrator will receive an email confirmation for the approved affiliation request.



**Figure 6.9:** Email Confirmation for Approved Affiliation Request.

6. After the submitter approves the affiliation request, the Administrator **must** assign NPI, Transaction and Claim Type permissions to complete the approval process or submitters will be unable to submit claims for the provider organization. Refer to the [User Permissions](#) section for instructions regarding assigning these permissions.

# Approve a Submitter Affiliation Request

1. Under the **Pending Requests** tab, select a submitter organization.

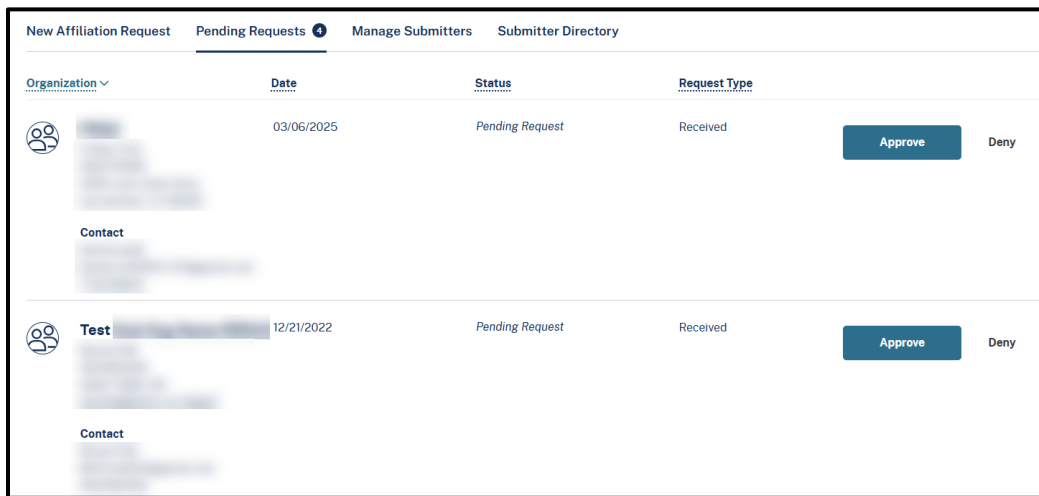


Figure 6.10: Pending Requests.

# Deny a Submitter Affiliation Request

1. Under the Pending Requests tab, select the submitter organization and select **Deny**.

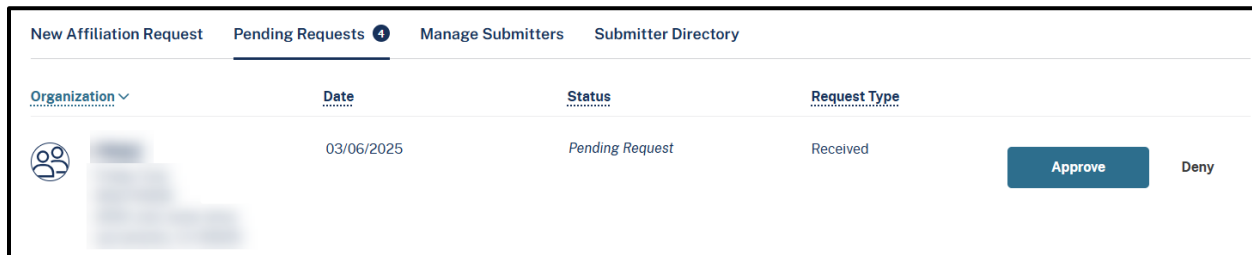


Figure 6.11: Deny Pending Requests.

2. A pop-up screen will appear asking, "Are you sure you want to deny this request?". Select **Deny** to remove the affiliation request.

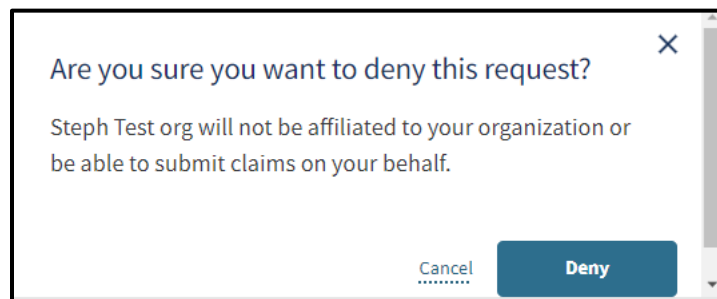
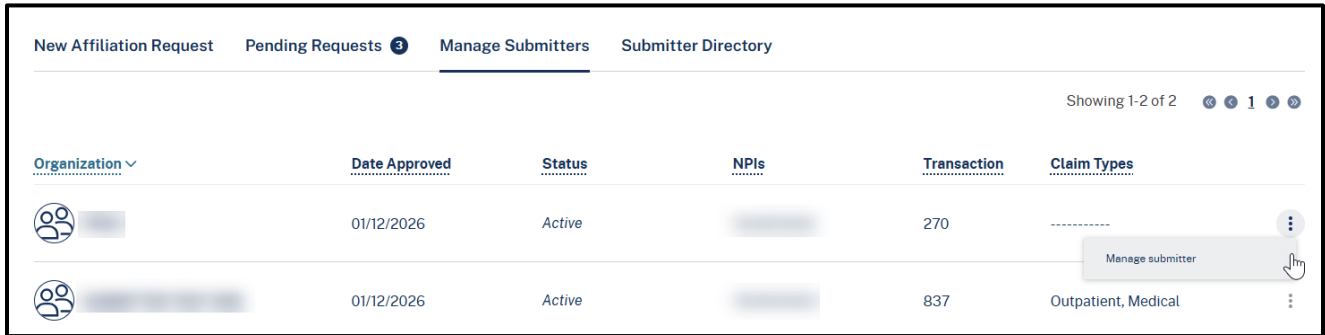








Figure 6.12: Deny Request Confirmation.

3. A notification will appear under the **Pending Requests** tab stating “Request successfully denied,” and the request will be removed.

## Manage Submitters

1. To manage a submitter organization’s permissions, select the **kebab menu** icon (  ) at the end of the row and select **Manage Submitter**.




Organization	Date Approved	Status	NPIs	Transaction	Claim Types	
	01/12/2026	Active		270	-----	 Manage submitter
	01/12/2026	Active		837	Outpatient, Medical	

**Figure 6.13:** Manage Submitters.

2. Select **Edit** on the far right of the **Provider Affiliations** area.

### Submitter Management and Permissions


[Remove submitter from organization](#)



## SUBMITTER TEST ORG

Submitter ID: [REDACTED]

<b>Organization Information:</b>	<b>Contact:</b>	<b>Affiliation Status:</b>	<b>Date Approved:</b>
[REDACTED]	[REDACTED]	Active	01/12/2026
[REDACTED]	[REDACTED]		<b>Last Login Date</b>
[REDACTED]	[REDACTED]		01/12/2026



### Provider Affiliations

[Edit](#)

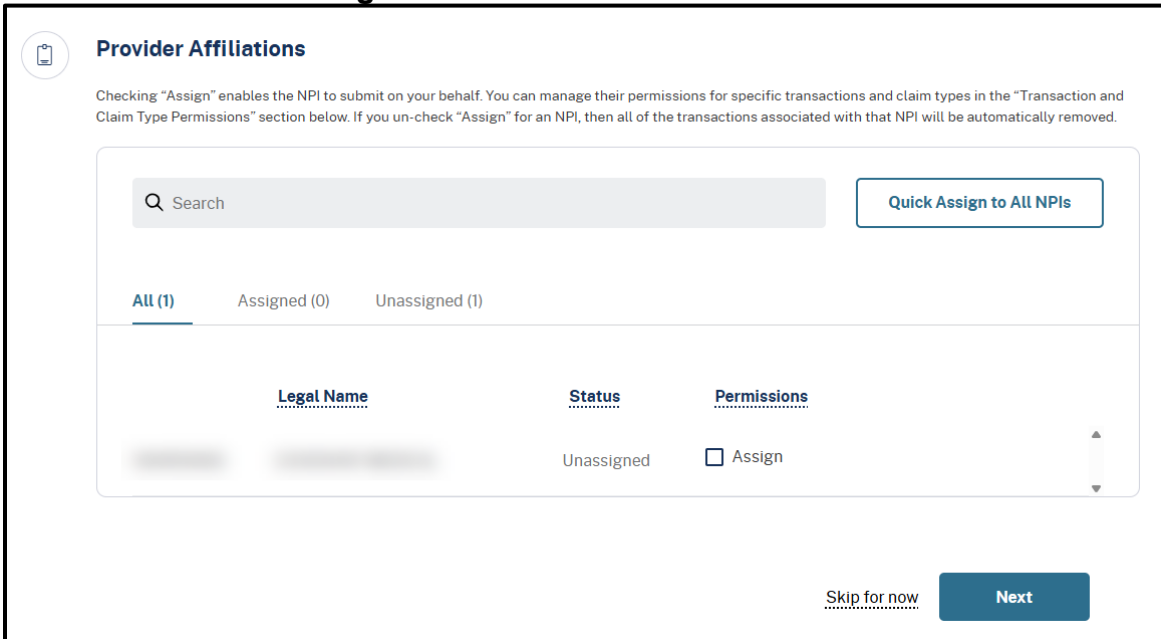
Checking "Assign" enables the NPI to submit on your behalf. You can manage their permissions for specific transactions and claim types in the "Transaction and Claim Type Permissions" section below. If you un-check "Assign" for an NPI, then all of the transactions associated with that NPI will be automatically removed.

[All \(1\)](#)   [Assigned \(1\)](#)   [Unassigned \(0\)](#)

<u>NPI</u>	<u>Legal Name</u>	<u>Status</u>
[REDACTED]	[REDACTED]	Assigned

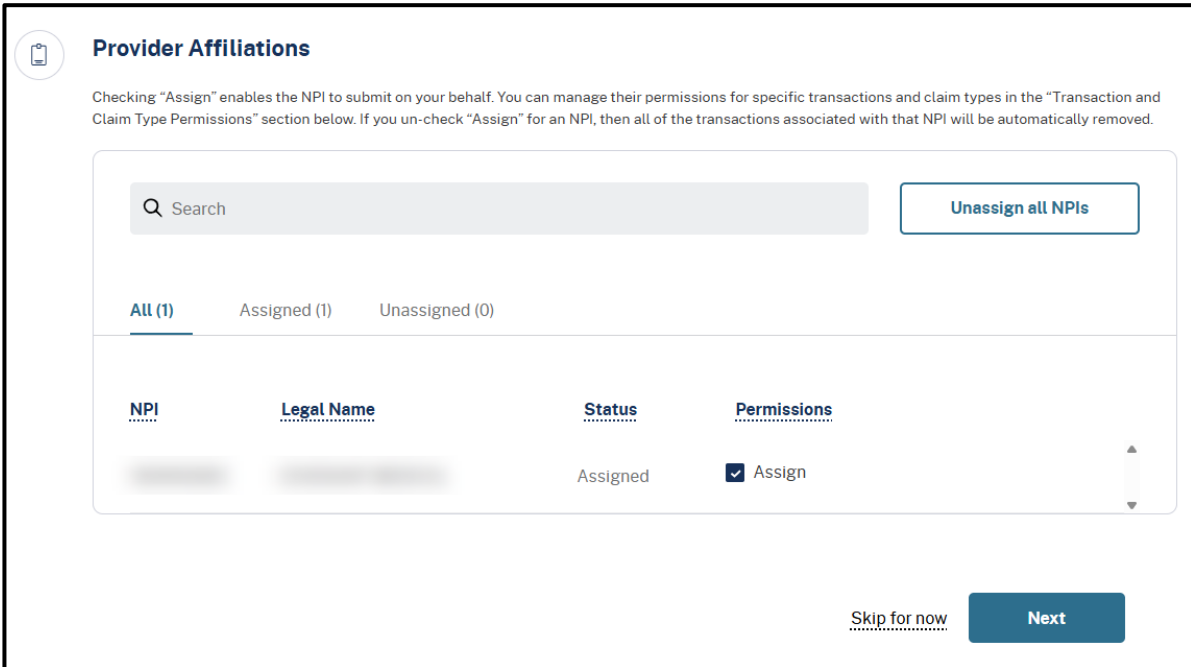
**Figure 6.14:** Submitter Management and Permissions.

- To assign NPI permissions to the submitter organization, select **Quick Assign to All NPIs** or select the **Assign** checkbox for the desired NPI.



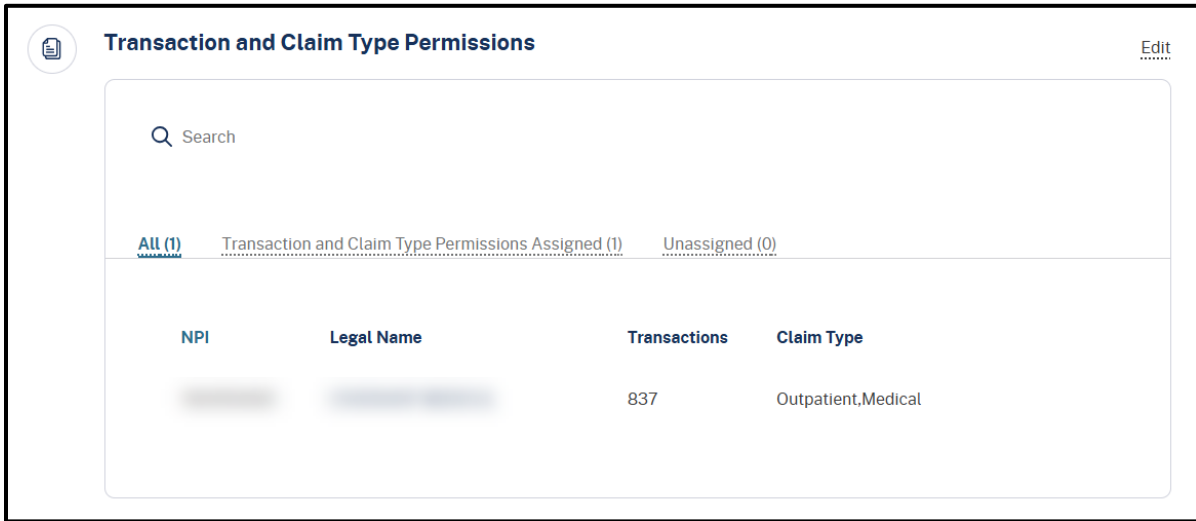
**Figure 6.15:** Provider Affiliations.

- Once an NPI is assigned, select **Next**.



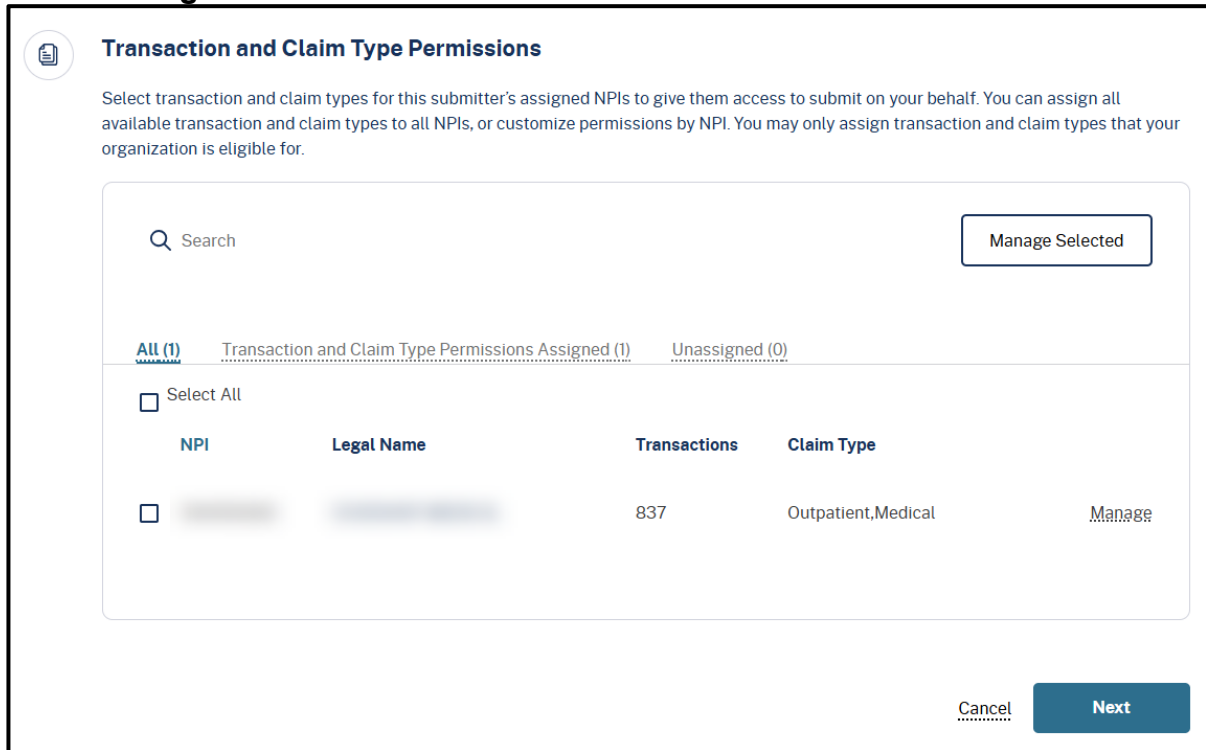
**Figure 6.16:** Assign NPI Permissions.

5. Select **Edit** on the far right of the **Transaction and Claim Type Permissions** area.



**Figure 6.17:** Transaction and Claim Type Permissions.

6. To manage **Transaction and Claim Type Permissions**, select **Manage Selected** or the **Manage** link.



**Figure 6.18:** Manage Selected NPIs.

7. Select the desired claim types to assign to the submitter organization, then select **Save**.

**Manage Transaction and Claim Type Permissions**

NPI [REDACTED]

The current transaction and claim permissions for the selected types are not eligible for every NPI. Eligibility is indicated by enabled and disabled text depending on the NPI.

- Assign All
- 837
- Inpatient
- Outpatient
- Medical**
- Long Term Care
- 270

**Note:** Removing the Medical claim type will terminate the ability to submit these claim types and also eliminate the ability to use the Internet Claim Submission (IPCS).

Cancel Save

**Figure 6.19:** Manage Transaction and Claim Type Permissions.

8. Administrators are also able to view the **Signed Agreement and Signatures** of the submitter and provider within **Manage Submitters**.

**View Signed Agreement and Signatures**

Submitter + Provider Affiliation Agreement

Mcpportal055  
Signed 02/07/2024

Signed 01/26/2024

View Agreement

**Figure 6.20:** View Signed Agreement and Signatures.

# Submitter Directory

Organization Administrators and assigned users have access to the Submitter Directory within Submitter Management. The directory contains the contact information and the approved submission capabilities of registered submitter organizations.

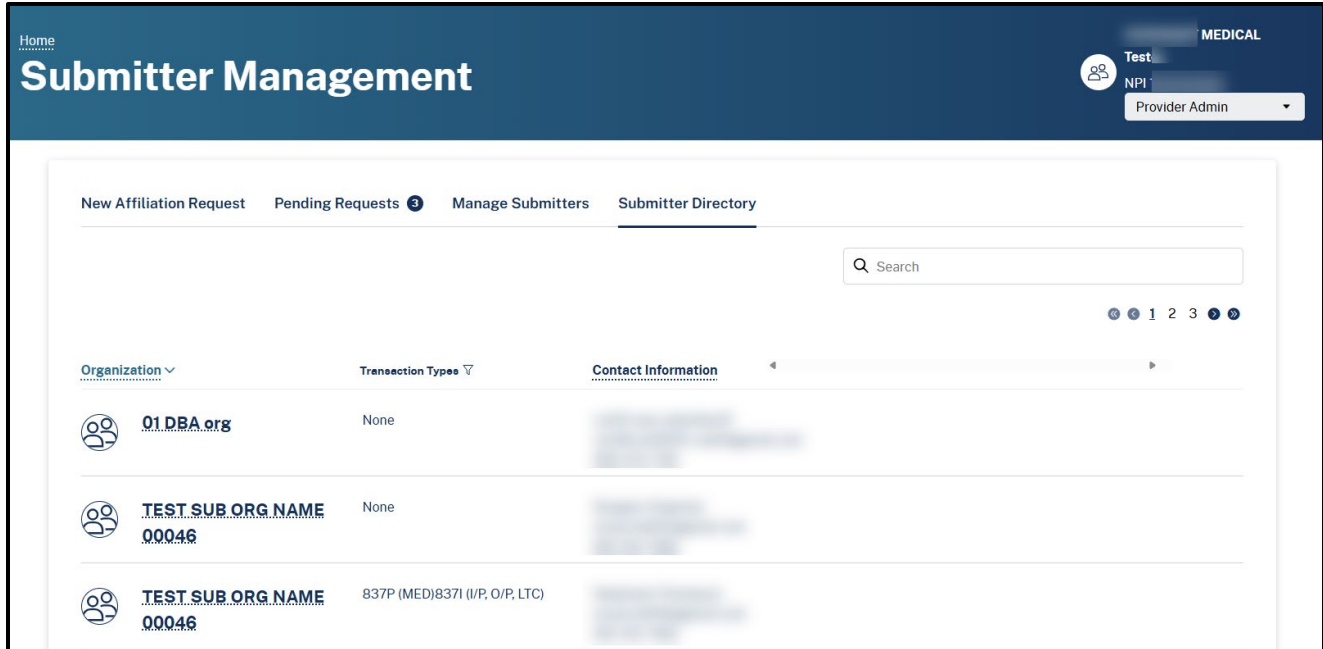


Figure 6.21: Submitter Directory.

# Navigating the Provider Portal

The Provider Portal consolidates Medi-Cal-related information for the user's organization into one location. The following sections provide details on how to use each of the Provider Portal areas.

## My Account

The **My Account** page will give users the ability to set or update their preferences by using the left navigation panel. This area allows users to modify account information such as business or cell phone numbers.

1. Select the **My Account** tab from any page in Provider Portal.



Figure 7.1: Select My Account.

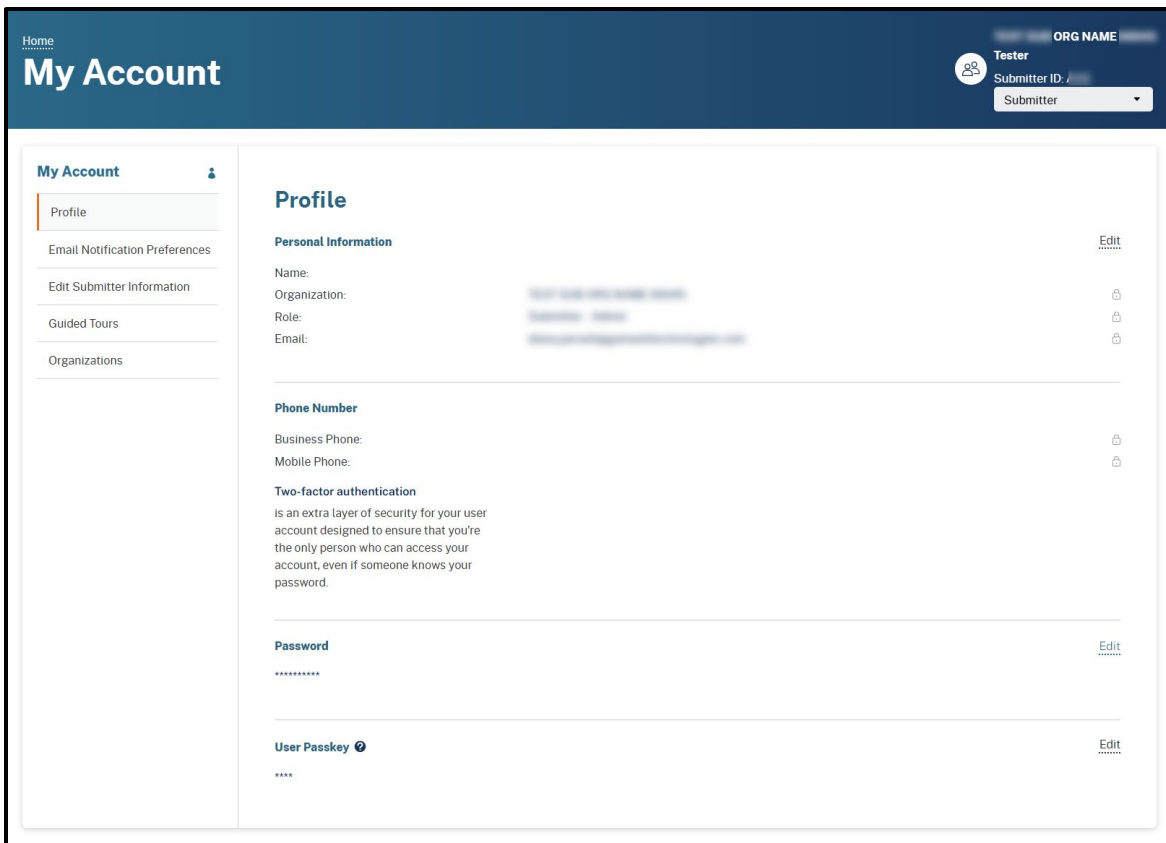


Figure 7.2: My Account Landing Page.

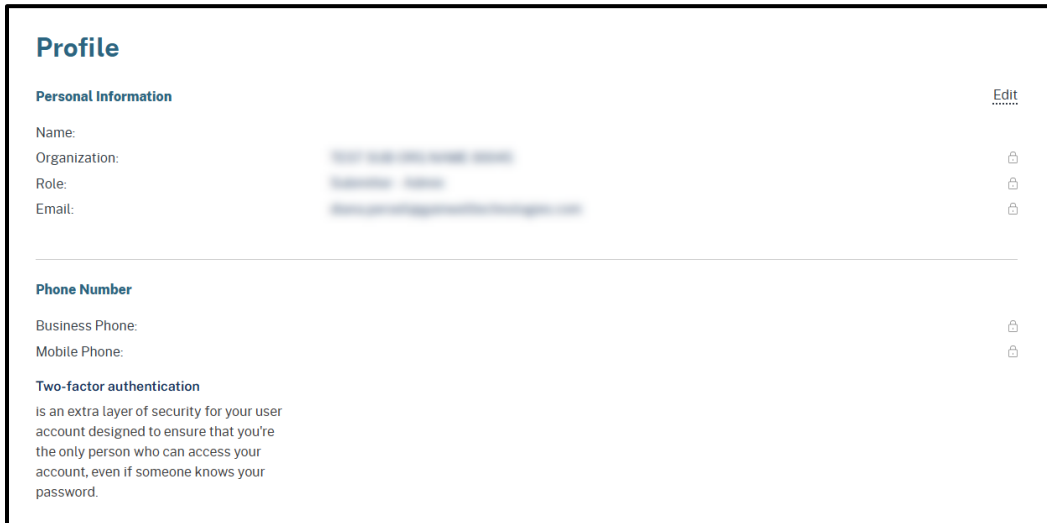
# Profile

The **Profile** area houses personal account information and notification preferences.

## Personal Information and Phone Number

1. Select the **Profile** tab on the left of the screen. Select the **Edit** hyperlink in line with the Personal Information section and follow the steps provided.

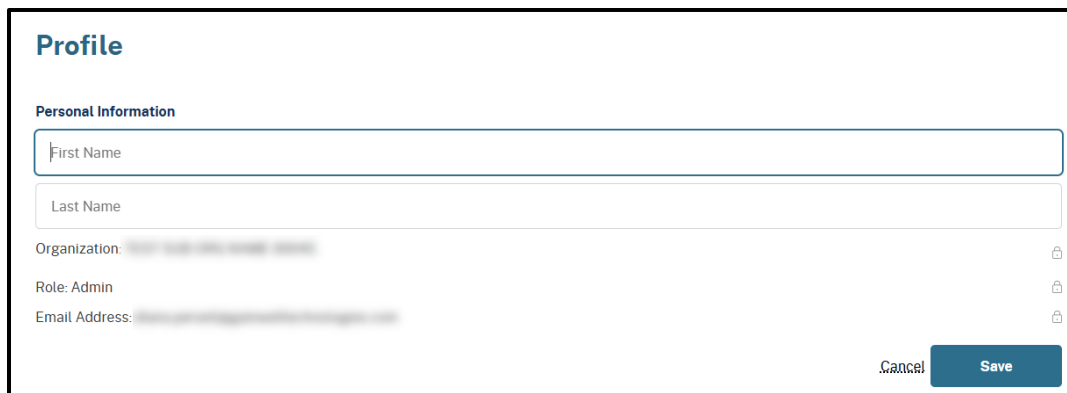
**Note:** The field opens allowing the user to edit the phone number. If the phone number selected is not assigned to a two-factor authentication and the user would like to use a two-factor authentication, select **Use this number for two-factor authentication**.



The screenshot shows the 'Profile' page with the following sections:

- Profile** (Title)
- Personal Information** (Section Header) with an **Edit** link to the right.
- Fields for Name, Organization, Role, and Email, each with a lock icon on the right.
- Phone Number** (Section Header)
- Fields for Business Phone and Mobile Phone, each with a lock icon on the right.
- Two-factor authentication** (Section Header) with a descriptive paragraph below it.


**Figure 7.3:** Edit Profile Information.



The screenshot shows the 'Profile' page with the following sections:

- Profile** (Title)
- Personal Information** (Section Header)
- Input fields for First Name and Last Name.
- Fields for Organization, Role (Admin), and Email Address, each with a lock icon on the right.
- Cancel** and **Save** buttons at the bottom right.

**Figure 7.4:** Edit Personal Information.

**Note:** The lock (  ) icon on the right-hand side of the field indicates that the field cannot be edited. These fields can only be edited by the Administrator who created the user profile. If a user is a member of multiple organizations, the user will not be able to edit the email address. The user must be deactivated from the organizations and re-added to the Portal as a new user with a new email address.

2. Select the **Edit** hyperlink to update the business phone number. This number can also be used for two-factor authentication. **Select Save.**

**Phone Number**

Business Phone:  [Edit](#)

Mobile Phone:

Use this number for two step authentication

[Cancel](#) [Save](#)

**Two-factor authentication**  
is an extra layer of security for your user account designed to ensure that you're the only person who can access your account, even if someone knows your password.

**Figure 7.5:** Edit Phone Number.

3. A confirmation appears indicating the updated information was successfully updated.

### Change a Password or Passkey

1. Select the **Profile** tab on the left of the screen. Select the **Edit** hyperlink in line with the Password or User Passkey section and follow the steps provided.

**Password** [Edit](#)

\*\*\*\*\*

**User Passkey** [Edit](#)

\*\*\*\*

**Figure 7.6:** Edit Passkey.

2. Enter a new four (4) digit passkey into the fields and select **Save Changes**. It is important to remember the passkey as it will be needed to reset passwords with help desk and for security verification.

**User Passkey**

Enter 4 digit User Passkey \*

.....

Retype 4 digit User Passkey \*

.....

[Cancel](#) [Save Changes](#)

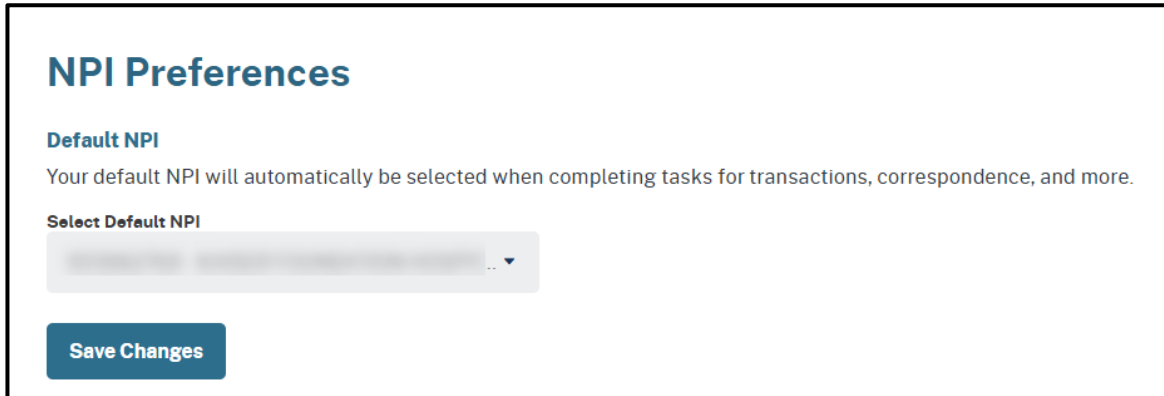
**Figure 7.7:** Enter New Passkey.

Once complete, a successfully updated user passkey message will appear.

## NPI Preferences

A default NPI will be automatically selected when completing tasks for transactions, correspondence and more.

1. To edit the NPI Preferences, a user can select a different NPI from the drop-down menu and then select **Save Changes**.



The screenshot shows a form titled "NPI Preferences". Under the heading "Default NPI", there is a text box explaining that the default NPI will be used for transactions, correspondence, and more. Below this is a "Select Default NPI" label followed by a greyed-out dropdown menu. At the bottom of the form is a blue "Save Changes" button.

**Figure 7.8:** NPI Preferences.

## Email Notification Preferences

Users automatically receive notifications in the Provider Portal.

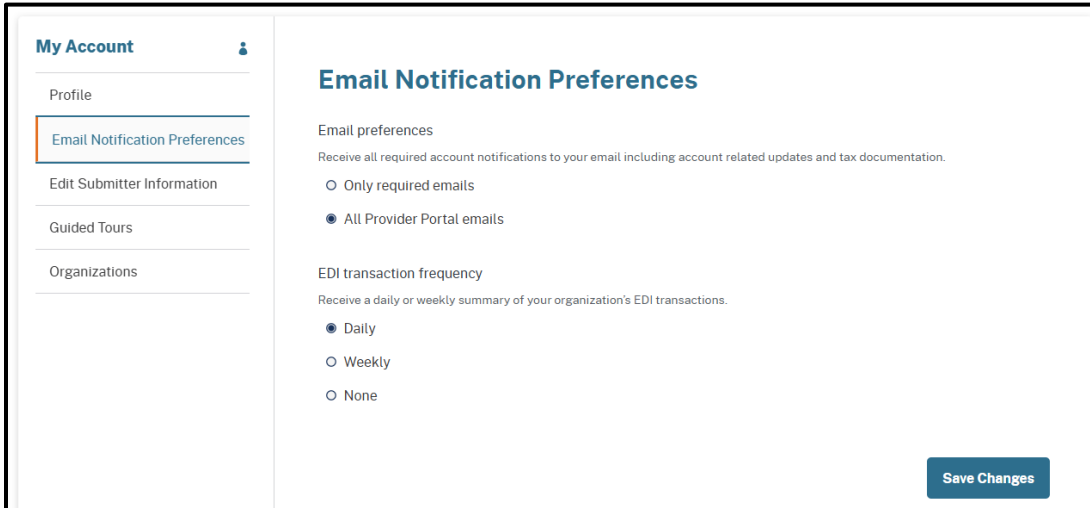
1. Select **My Account**



**Figure 7.8:** Select My Account.

2. In the **Email Notification Preferences** section, users set **Email Preferences** by selecting only required emails or all Provider Portal emails, and set the **EDI transactions frequency** to Daily, Weekly or None

3. Select **Save Changes** at the bottom of the page to finish updating preferences. A confirmation appears indicating that the preferences are saved.

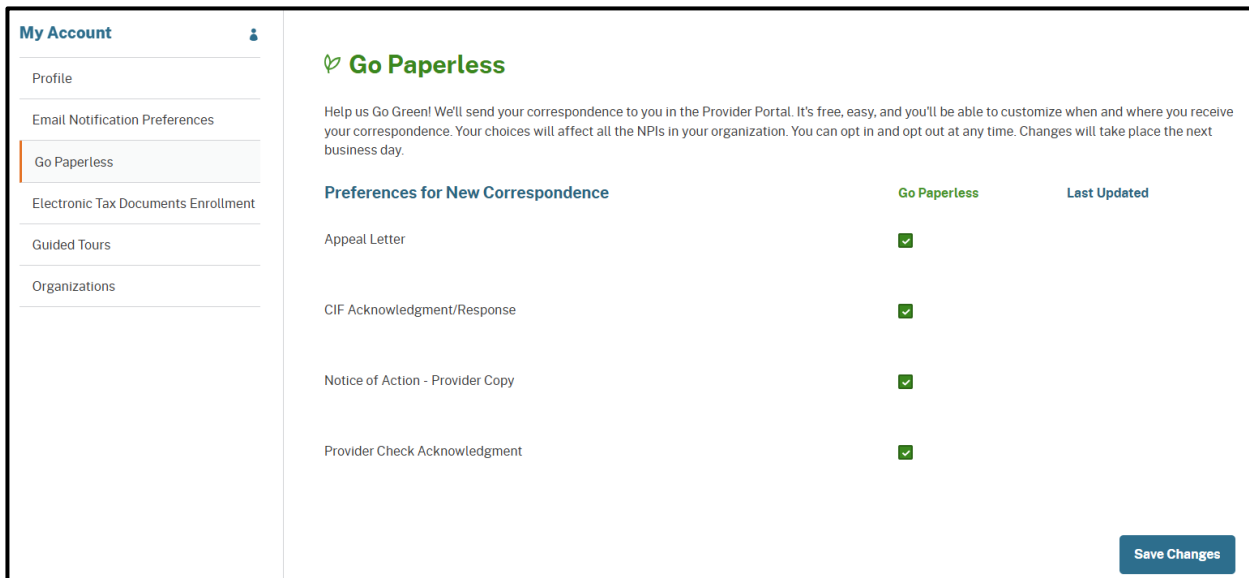


**Figure 7.10:** Notification Frequency.

## Going Paperless

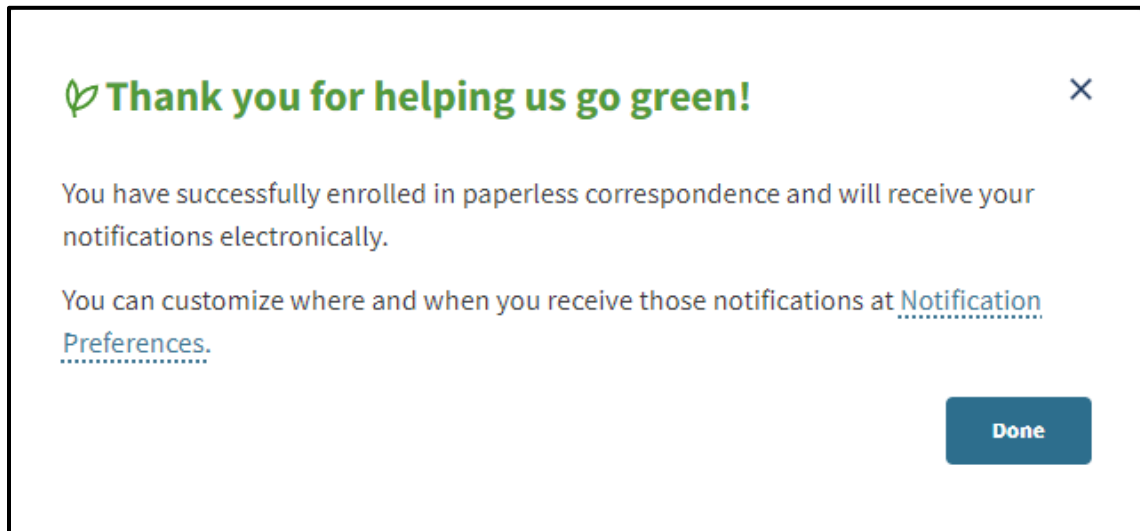
The Provider Portal is designed to help organizations go green and reduce the use of paper for communications. An Administrator of an organization can enroll in paperless communications by completing the following:

1. Under My Account, select **Go Paperless** from the left navigation. Check the box(es) next to the desired correspondence. Select **Save Changes** to set this preference.



**Figure 7.11:** Go Paperless Page.

A confirmation screen appears. The user is now enrolled in paperless communications.



**Figure 7.12:** Go Paperless Enrollment Confirmation.

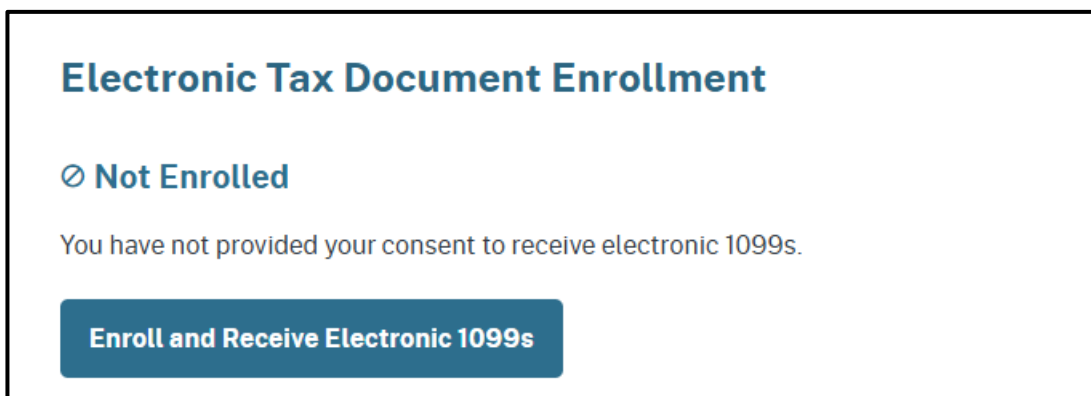
## Edit Tax Document Enrollment

The Provider Portal allows users to enroll in electronic communications for their tax documents. If enrolled, the user will receive 1099s through the Portal instead of by mail.

Initial settings for this feature are set by the Administrator of the organization. To enroll or withdraw enrollment, refer to the following:

### Enrolling

1. In My Account, select the **Electronic Tax Documents Enrollment** from the navigation options.
2. Enrollment status of Not Enrolled will display. Select the **Enroll and Receive Electronic 1099s** button.



**Figure 7.13:** Edit Electronic Tax Documents Enrollment.

3. Read the Electronic 1099 Consent Agreement, and then select the **I Have Read and Agree to The Above** button.

**Electronic 1099 Consent Agreement**

I acknowledge and agree to the following on behalf of my organization:

1. You agree to receive all 1099s for your organization electronically and understand you will not receive a paper copy by mail once enrolled in electronic 1099s.
2. DHCS will continue to provide a paper copy by mail if you do not consent to receive electronic 1099s or if you withdraw your consent.
3. Consent may be withdrawn at any time within your Provider Portal account settings.
4. If you wish to receive a paper copy, you may call the Provider Portal Support Line and request that one be sent to you.
5. If your Provider Organization is dis-enrolled from Medi-Cal, an electronic 1099 will not be generated. Any pending 1099s will be delivered via mail to your address on file. Requests to update your address information can be completed by contacting the Telephone Service Center.
6. 1099s will be available for two years, after which they will be removed from Provider Portal. If you wish to receive a copy of a 1099 dated prior to the last two years, you may call the Provider Portal Support Line and request that a copy be mailed to you.
7. To access your 1099s electronically you must have an internet enabled device with access to DHCS Medi-Cal compatible browsers capable of downloading, saving, and printing an Adobe .PDF file. To view the Medi-Cal website compatible browsers, please go to the [Web Tool Box](#).
8. If you withdraw your consent, you will no longer have access to past or future electronic 1099s until you re-enroll and DHCS will resume providing a paper copy for the upcoming fiscal year.

**Figure 7.14:** Electronic 1099 Consent Agreement.

4. Once selected, the user is successfully enrolled to receive electronic 1099s. A confirmation message appears at the top of the screen. Enrollment status is always available on the Electronic Tax Documents Enrollment page where it displays *Enrolled*.

## Withdrawing Enrollment

The Electronic Tax Documents Enrollment page displays current enrollment status.

1. Select the **Withdraw Consent and Receive Paper 1099s** button.

**Electronic Tax Document Enrollment**

**Enrolled**

You are enrolled to receive your 1099s electronically through Provider Portal.

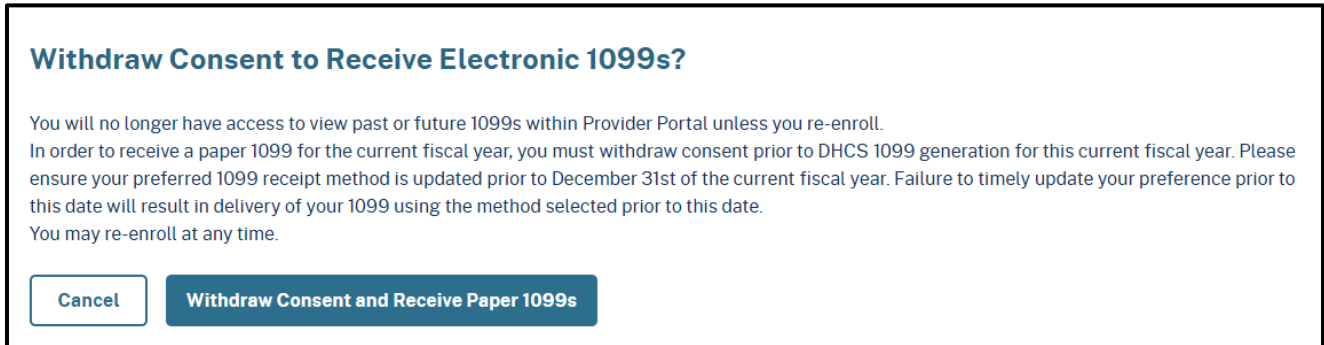
If you would like to withdraw consent, please unenroll below. All tax documents for upcoming tax years will be sent in paper form only. You may re-enroll in electronic 1099s at any time.

Date Enrolled:  
11/12/

Enrolled by:

**Figure 7.15:** Electronic 1099 Consent Withdrawal.

2. A page appears verifying that the user would like to receive paper 1099s. Select the **Withdraw Consent and Receive Paper 1099s** button to confirm disenrollment. A confirmation message appears at the top of the page.



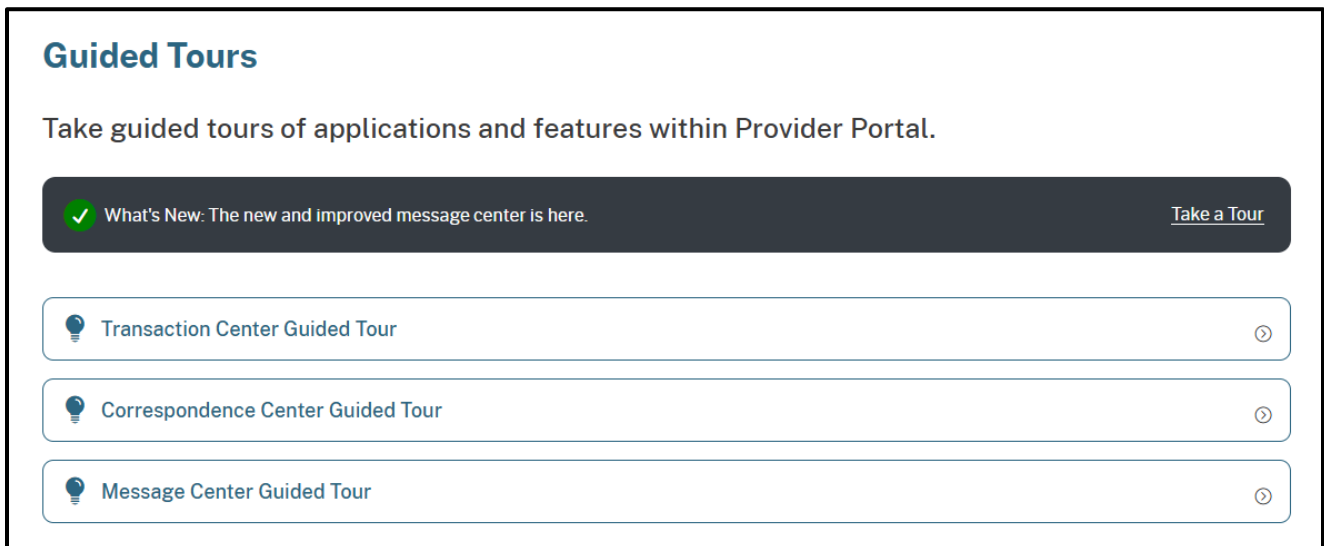
**Figure 7.16** Withdraw consent to receive electronic 1099s.

3. Once confirmed, the user is successfully disenrolled from receiving electronic 1099s. The user may check enrollment status on the Electronic Tax Documents Enrollment page where it displays *Not Enrolled*.

## Guided Tours

Guided tours are available within Provider Portal to point out key features of the applications.

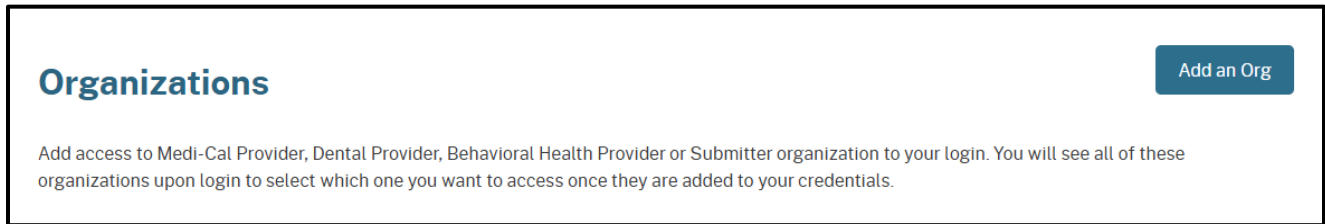
1. Access **Guided Tours** anytime through the Guided Tours tab in My Account.



**Figure 7.17:** Guided Tours.

## Organizations

2. Select **Add an Org** to provide access to providers and submitters to the administrator's login credentials.



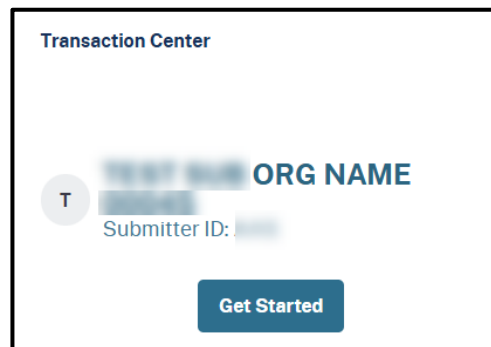
**Figure 7.18:** Add New Organization.

Refer to the Add an Enrolled Provider Organization section of this user guide for step-by-step instructions.

## Transaction Center

Provider Portal users may access the Transaction Center by a secure single sign-on.

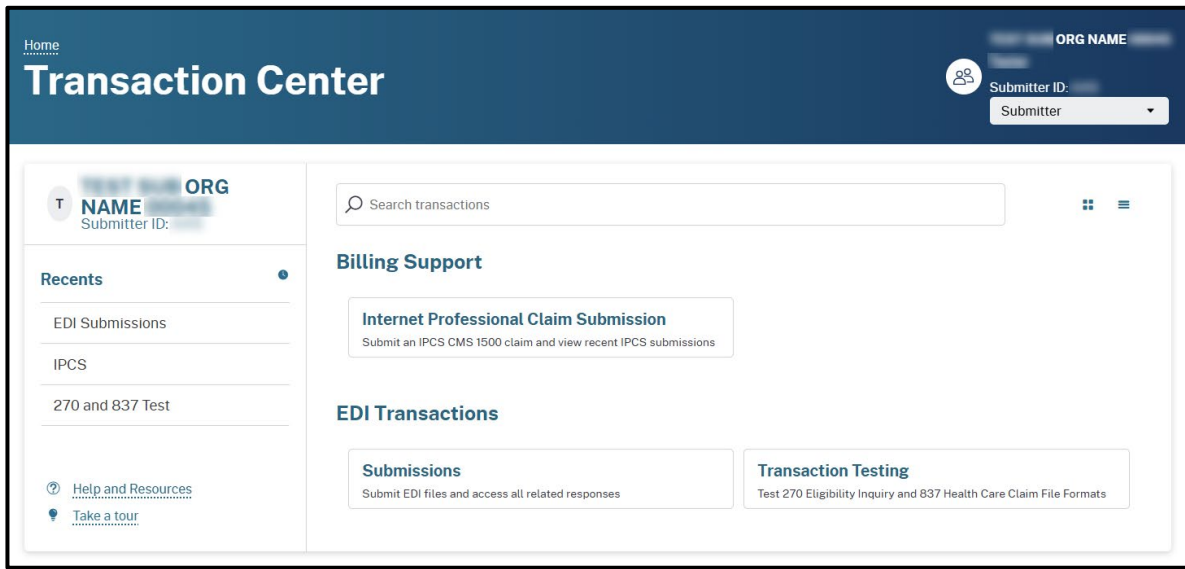
1. Select the **Get Started** button within the Transaction Center tile on the Provider Portal Dashboard.



**Figure 7.19:** Transaction Center Tile.

Transactions based on login credentials are displayed in the main section of the page.

2. Select the **transaction tile** to begin.

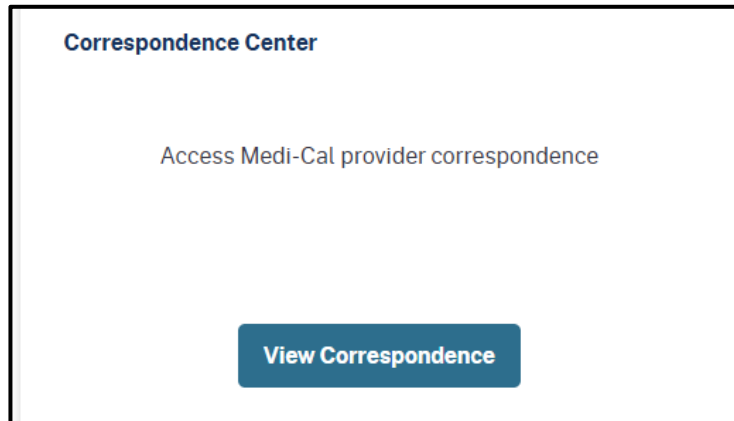


**Figure 7.20:** Transaction Center.

# Correspondence Center

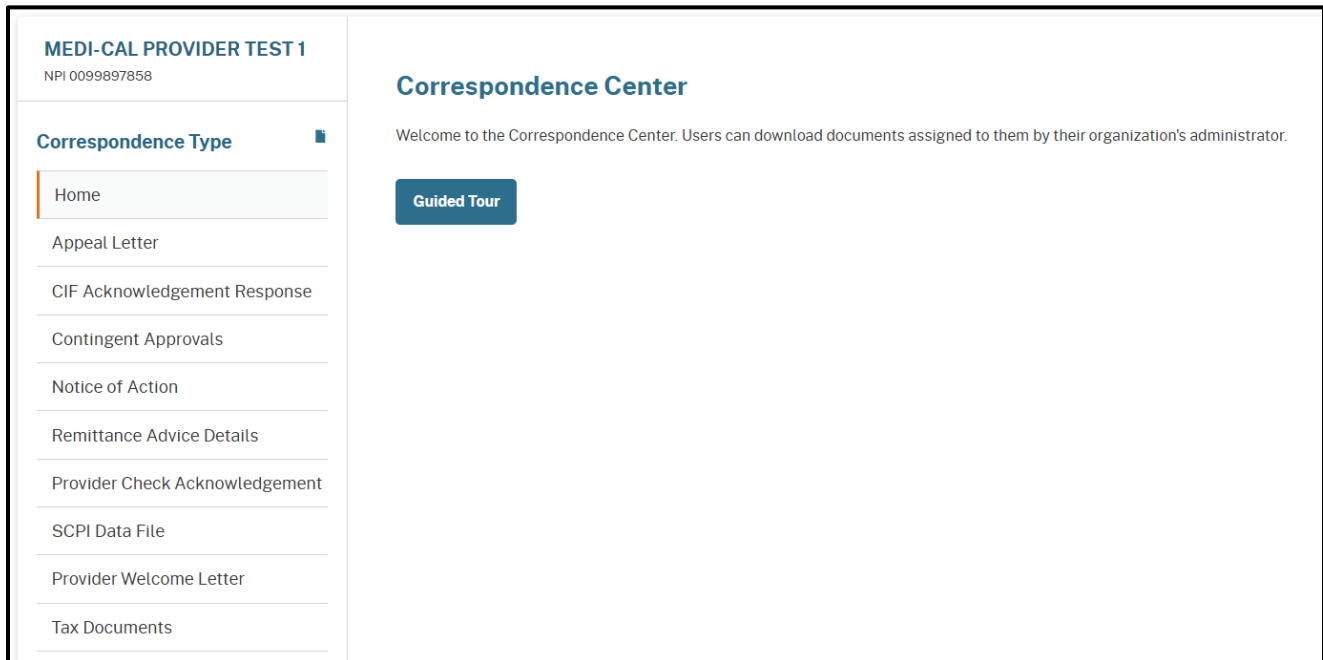
The **Correspondence Center** contains with the most recent updates and available documents. The types of correspondence available to providers may be different depending upon the organization type.

1. Select **View Correspondence**.



**Figure 7.21:** Correspondence Center Tile.

2. Access the **Guided Tour** from the Home page of Correspondence Center.



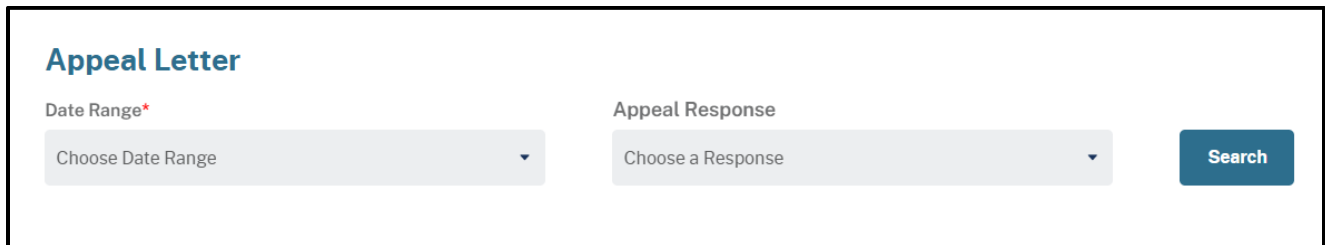
**Figure 7.22:** Correspondence Center Home.

## Types of Correspondence

The **Correspondence Center** allows access to all organizations' correspondence based on NPI access. When completing search criteria fields for correspondence, fields with a red asterisk (\*) must be filled in to access search results.

### Appeal Letter

1. Use the Date Range (within one year) and Appeal Response fields then select **Search**.

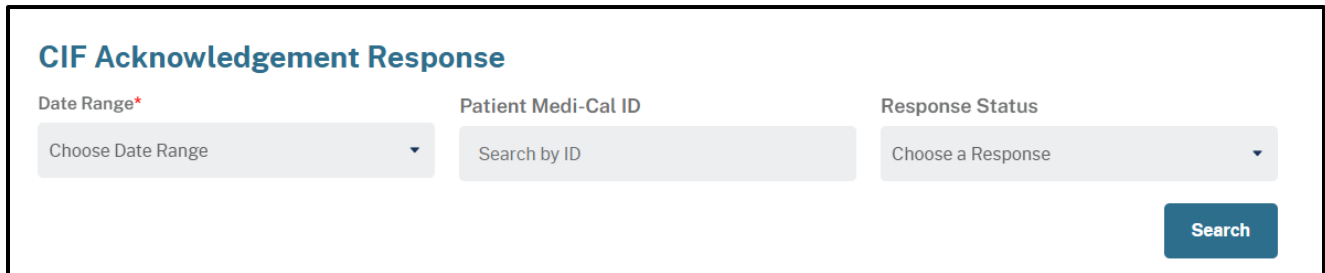


The screenshot shows a search form titled "Appeal Letter". It contains three main input areas: "Date Range\*" with a dropdown menu showing "Choose Date Range", "Appeal Response" with a dropdown menu showing "Choose a Response", and a blue "Search" button.

**Figure 7.23:** Appeal Letter Search Criteria.

### CIF Acknowledgement Response

1. Use the Date Range (last 7, 14, 30 days or custom), Patient Medi-Cal ID, and Response Status fields then select **Search**.



The screenshot shows a search form titled "CIF Acknowledgement Response". It contains three main input areas: "Date Range\*" with a dropdown menu showing "Choose Date Range", "Patient Medi-Cal ID" with a text input field containing "Search by ID", and "Response Status" with a dropdown menu showing "Choose a Response". A blue "Search" button is located at the bottom right.

**Figure 7.24:** CIF Acknowledgement Response Search Criteria.

### Contingent Approvals

The list of Contingent Approvals is organized by Owner Number, Email Address Program Type and Date Email Sent. Owner Number can be sorted in order. Only enrolled Qualified Providers (QPs) in Children's Presumptive Eligibility (CPE) are eligible to access Contingent Approval notices.

1. Check one or more of the **check boxes** to download the approval.

The screenshot shows a web interface with a sidebar on the left and a main content area. The sidebar, titled 'Correspondence', lists various document types: Home, Appeal Letter, CIF Acknowledgement/Response, **Contingent Approvals** (highlighted), Notice of Action - Provider Copy, Provider Check Acknowledgement, Provider Welcome Letter, Remittance Advice Details, SCPI Data File, and Tax Documents. The main content area is titled 'Contingent Approvals' and contains a table with the following columns: Owner Number, Email Address, Program Type, and Date Email Sent. There are six rows of data, each with a checkbox in the 'Owner Number' column and a download icon in the 'Date Email Sent' column.

Owner Number	Email Address	Program Type	Date Email Sent
<input type="checkbox"/> 01	alex.taylor@grantmed.org	Children's Presumptive...	09/05/2025
<input type="checkbox"/> 02	lisa.nguyen@grantmed.org	Hospital Presumptive...	09/05/2025
<input type="checkbox"/> 03	mike.jones@grantmed.org	Hospital Presumptive...	09/05/2025
<input type="checkbox"/> 04	david.kim@grantmed.org	Hospital Presumptive...	09/05/2025
<input type="checkbox"/> 05	emily.clark@grantmed.org	Presumptive Eligibility for...	09/05/2025
<input type="checkbox"/> 06	jon.williams@grantmed.org	Presumptive Eligibility for...	09/05/2025

**Figure 7.25:** Contingent Approvals Results.

2. Filter by Program Type to narrow results by program. Select the column header **Program Type**, then check the box of the desired program and select **Apply**.

This screenshot shows the same 'Contingent Approvals' table as Figure 7.25, but with a dropdown menu open for the 'Program Type' column. The dropdown menu lists three options: 'Children's Presumptive Eligibility', 'Hospital Presumptive Eligibility', and 'Presumptive Eligibility for Pregnant People'. At the bottom of the dropdown is an 'Apply' button. The table rows are partially obscured by the dropdown menu.

Owner Number	Email Address	Program Type	Date Email Sent
<input type="checkbox"/> 01		<input type="checkbox"/> Children's Presumptive Eligibility	09/05/2025
		<input type="checkbox"/> Hospital Presumptive Eligibility	
<input type="checkbox"/> 02		<input type="checkbox"/> Presumptive Eligibility for Pregnant People	09/05/2025
		<b>Apply</b>	
<input type="checkbox"/> 03	ed.org	Presumptive...	09/05/2025

**Figure 7.26:** Program Type Options.

## Notice of Action

1. Use the Date Range (last 7, 14, 30 days or custom) then select **Search**.



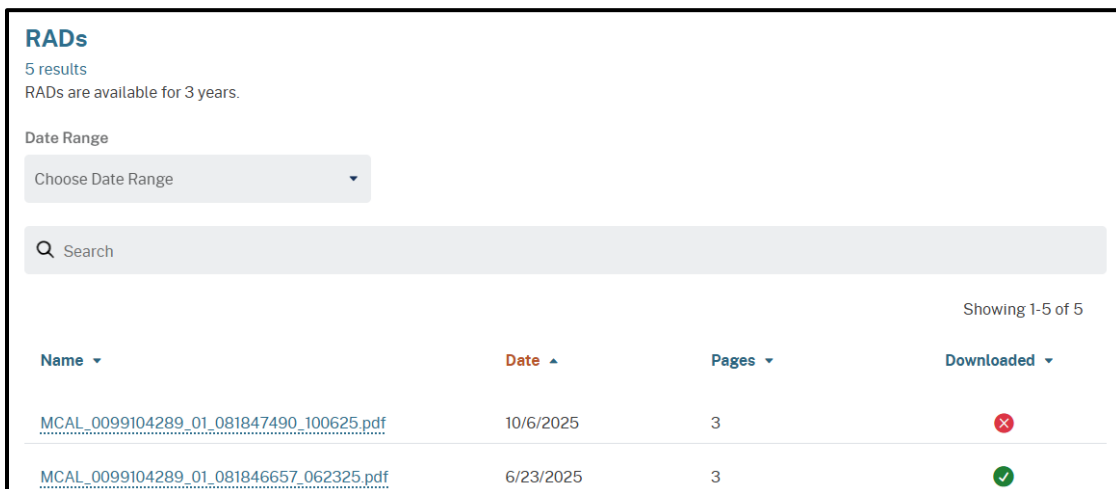
The screenshot shows a search interface for 'Notice of Action'. It features a title 'Notice of Action' in blue. Below the title is a 'Date Range\*' label and a dropdown menu with the text 'Choose Date Range'. A blue 'Search' button is located in the bottom right corner.

Figure 7.27: Notice of Action Search Criteria.

## Remittance Advice Details (RADs)

A list of available RADs is organized by **Name**, **Date** and **Number of Pages**. Previously downloaded RADs are identified by a green “check mark” and those not downloaded display a red “X” icon.

1. Use the Date Range (last 7, 14, 30 days or custom) and the search field to refine results. **Note:** RADs are available for three years.




The screenshot shows the 'RADs' search results page. It includes a title 'RADs', '5 results', and a note 'RADs are available for 3 years.'. There is a 'Date Range' dropdown menu and a search bar with a magnifying glass icon. Below the search bar, it says 'Showing 1-5 of 5'. The results are displayed in a table with columns: Name, Date, Pages, and Downloaded.

Name	Date	Pages	Downloaded
<a href="#">MCAL_0099104289_01_081847490_100625.pdf</a>	10/6/2025	3	✗
<a href="#">MCAL_0099104289_01_081846657_062325.pdf</a>	6/23/2025	3	✓

Figure 7.28: RAD Results and Search Criteria.

## Provider Check Acknowledgement

1. Use the Date Range (last 7, 14, 30 days or custom) then select **Search**.




The screenshot shows a search interface for 'Provider Check Acknowledgement'. It features a title 'Provider Check Acknowledgement' in blue. Below the title is a 'Date Range\*' label and a dropdown menu with the text 'Choose Date Range'. A blue 'Search' button is located in the bottom right corner.

Figure 7.29 Provider Check Acknowledgment Search Criteria.

## Supplemental Claims Payment Information (SCPI) Data File

1. Use the Date Range (last 7, 14, 30 days or custom) then select **Search**.

**Note:** Only the past six weeks of SCPI are available through the Portal.



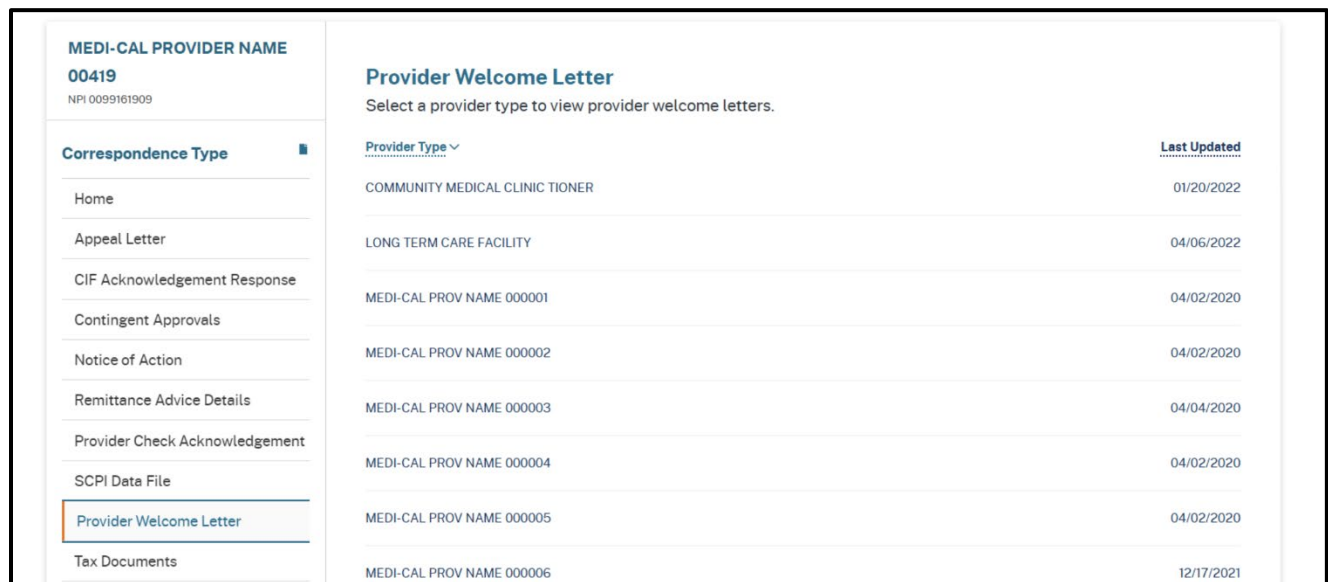
The screenshot shows a web interface titled "SCPI Data File". Below the title, there is a "Date Range\*" label and a dropdown menu with the text "Choose Date Range". To the right of the dropdown is a blue button labeled "Search".

**Figure 7.30:** Provider Check Acknowledgment Data Range.

## Provider Welcome Letter

Provider welcome letters contain information about NPIs, and provider communities related to the organization. Welcome Letters are listed by **Provider Type** and the **Last Updated** date.

1. In the result of multiple provider types, select one from the list.



The screenshot shows a web interface titled "Provider Welcome Letter". On the left, there is a sidebar with a "Correspondence Type" menu. The main content area has a "Provider Type" dropdown and a table of providers. The table has columns for "Provider Type" and "Last Updated".

Provider Type	Last Updated
COMMUNITY MEDICAL CLINIC TIONER	01/20/2022
LONG TERM CARE FACILITY	04/06/2022
MEDI-CAL PROV NAME 000001	04/02/2020
MEDI-CAL PROV NAME 000002	04/02/2020
MEDI-CAL PROV NAME 000003	04/04/2020
MEDI-CAL PROV NAME 000004	04/02/2020
MEDI-CAL PROV NAME 000005	04/02/2020
MEDI-CAL PROV NAME 000006	12/17/2021

**Figure 7.31:** List of Providers Type.

- All available welcome letters are listed by **Name**, **NPI**, **Service Location** and **Date** created. Select the letter from the list to view the full letter.

<p><b>MEDI-CAL PROVIDER NAME</b> 00419 NPI 0099161909</p> <p><b>Correspondence Type</b></p> <ul style="list-style-type: none"> <li>Home</li> <li>Appeal Letter</li> <li>CIF Acknowledgement Response</li> <li>Contingent Approvals</li> <li>Notice of Action</li> <li>Remittance Advice Details</li> <li>Provider Check Acknowledgement</li> <li>SCPI Data File</li> <li><b>Provider Welcome Letter</b></li> <li>Tax Documents</li> </ul>	<p><b>Provider Welcome Letter</b> COMMUNITY MEDICAL CLINIC TIONER</p> <table border="1"> <thead> <tr> <th>Name</th> <th>NPI</th> <th>Service Location</th> <th>Date</th> </tr> </thead> <tbody> <tr> <td>Provider Welcome Letter</td> <td>0099097830</td> <td>216 AOKKVQZTS SGQR</td> <td>01/19/2022</td> </tr> <tr> <td>Provider Welcome Letter</td> <td>0099097830</td> <td>216 AOKKVQZTS SGQR</td> <td>01/20/2022</td> </tr> <tr> <td>Provider Welcome Letter</td> <td>0099097830</td> <td>830 STILLWATER ROAD</td> <td>04/02/2020</td> </tr> <tr> <td>Provider Welcome Letter</td> <td>0099097830</td> <td>1565 MIDDLE LANE</td> <td>04/06/2022</td> </tr> <tr> <td>Provider Welcome Letter</td> <td>0099097830</td> <td>2000 EVERGREEN ST</td> <td>11/21/2024</td> </tr> <tr> <td>Provider Welcome Letter</td> <td>0099104289</td> <td>830 STILLWATER ROAD</td> <td>04/02/2020</td> </tr> <tr> <td>Provider Welcome Letter</td> <td>0099161909</td> <td>830 STILLWATER ROAD</td> <td>04/04/2020</td> </tr> <tr> <td>Provider Welcome Letter</td> <td>0099212421</td> <td>216 AOKKVQZTS SGQR</td> <td>01/19/2022</td> </tr> </tbody> </table>	Name	NPI	Service Location	Date	Provider Welcome Letter	0099097830	216 AOKKVQZTS SGQR	01/19/2022	Provider Welcome Letter	0099097830	216 AOKKVQZTS SGQR	01/20/2022	Provider Welcome Letter	0099097830	830 STILLWATER ROAD	04/02/2020	Provider Welcome Letter	0099097830	1565 MIDDLE LANE	04/06/2022	Provider Welcome Letter	0099097830	2000 EVERGREEN ST	11/21/2024	Provider Welcome Letter	0099104289	830 STILLWATER ROAD	04/02/2020	Provider Welcome Letter	0099161909	830 STILLWATER ROAD	04/04/2020	Provider Welcome Letter	0099212421	216 AOKKVQZTS SGQR	01/19/2022
Name	NPI	Service Location	Date																																		
Provider Welcome Letter	0099097830	216 AOKKVQZTS SGQR	01/19/2022																																		
Provider Welcome Letter	0099097830	216 AOKKVQZTS SGQR	01/20/2022																																		
Provider Welcome Letter	0099097830	830 STILLWATER ROAD	04/02/2020																																		
Provider Welcome Letter	0099097830	1565 MIDDLE LANE	04/06/2022																																		
Provider Welcome Letter	0099097830	2000 EVERGREEN ST	11/21/2024																																		
Provider Welcome Letter	0099104289	830 STILLWATER ROAD	04/02/2020																																		
Provider Welcome Letter	0099161909	830 STILLWATER ROAD	04/04/2020																																		
Provider Welcome Letter	0099212421	216 AOKKVQZTS SGQR	01/19/2022																																		

**Figure 7.32: Welcome Letter List.**

### Tax Documents

- Select **Tax Year**, **Document Type** and **NPI** then select **Search**. The last two tax years and 1099s are currently available. Refer to the Edit Tax Document Enrollment section of this user guide for more information.

**Tax Documents**

Tax Year\*      Document Type      NPI\*

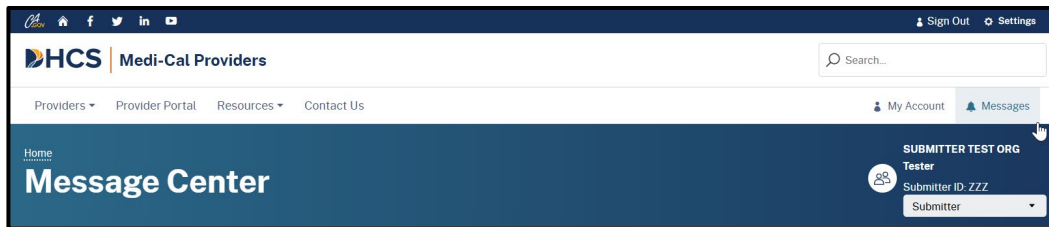
2024      1099      Choose an NPI

**Search**

**Figure 7.33: Tax Documents Search.**

# Message Center

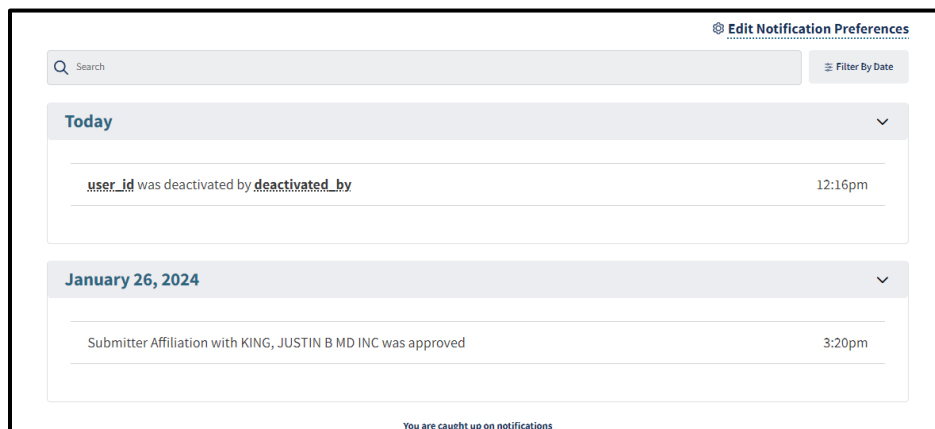
The Message Center contains notifications and messages and can be accessed from anywhere within the Provider Portal. If there are new messages or notifications a “dot” will appear next to the bell (🔔) icon. To see all notifications, select **Messages**.



**Figure 7.34:** Messages Tab.

A page appears with all past and current notifications. Past notifications can be viewed by using the search bar, or the **Filter By Date** feature.

1. To use the filter by date option, select the **Filter By Date** menu and enter the desired date range.
2. Select **Edit Notification Preferences** to add email notifications and adjust their frequency.



**Figure 7.35:** Notifications.

## Edit Email Notification Preferences

Users automatically receive notifications in the Provider Portal through the **Notifications** page. Users can get email and Portal notifications through the Notification Preferences page. Each email correspondence can be set for a desired frequency.

1. To add an email notification, select the **check box** in line with the correspondence.

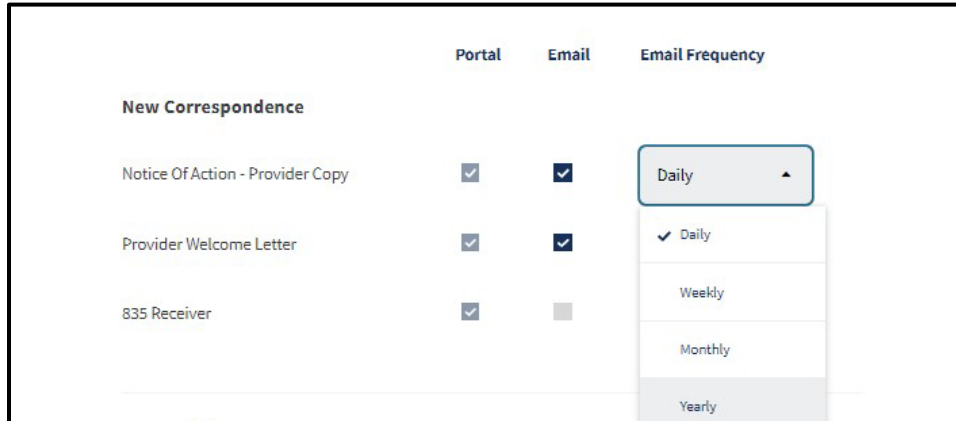
The screenshot displays the 'Notification Preferences' interface. It is organized into three main sections: 'New Correspondence', 'User Activity', and 'Password'. Each section contains a list of notification items with columns for 'Portal', 'Email', and 'Email Frequency'. A 'Save Changes' button is located at the bottom right.

	Portal	Email	Email Frequency
<b>New Correspondence</b>			
Notice Of Action - Provider Copy	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Daily
Provider Welcome Letter	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
835 Receiver	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Daily
<b>User Activity</b>			
Notify me when a user downloads or views correspondence in my organization	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Weekly
Notify me when a user in my organization downloads a document containing sensitive information	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Daily
Notify me when a password for a user in my organization is about to expire	<input checked="" type="checkbox"/>	<input type="checkbox"/>	5 Days Before
<b>Password</b>			
Notify me when my password is about to expire	<input checked="" type="checkbox"/>	<input type="checkbox"/>	5 Days Before
Notify me when my password has been reset	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Always

**Save Changes**

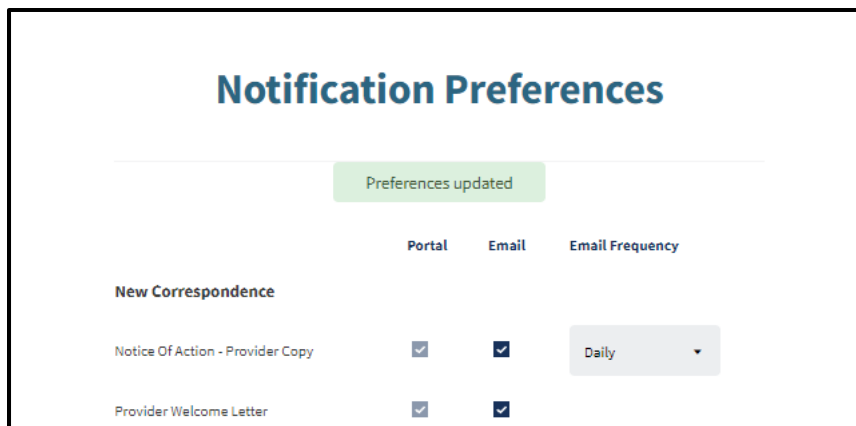
**Figure 7.36:** Edit Notification Preferences.

- To change the frequency of notification, select the **Notification Frequency** dropdown menu next to the specific notification to update the setting.



**Figure 7.37:** Edit Notification Frequency.

- Select **Save Changes** to finish updating preferences. A confirmation appears indicating that the settings are saved.



**Figure 7.38:** Notification Preference Successfully Updated.

# Change Summary

Version Number	Date	Description	Notes/Comments
1.0	April 19, 2023	Associated with SDN 20015B	Updated screenshots to match Medi-Cal Provider Portal functions.
1.1	July 28, 2023	Associated with SDN 20015B	Updated screenshots and instructions to include 835 Receiver Management functions. Updated formatting.
1.2	March 15, 2024	Associated with SDN 20015B	Updated screenshots to match the new DHCS rebranding and the Transaction Center functions.
1.3	May 2024	Associated with SDNs 20015B and 23036	Updated screenshots to match the dashboard changes in the Provider Portal and the DHCS logo on the cover page. Update formatting.
1.4	August 2024	Associated with OIL 101-24	Rebranding changes for PE4PW to PE4PP
1.5	September 2024	Associated with SDN 20015B	Updated screenshot to include the new Passkey and Unlock Password features. Update formatting.
1.6	September 2025	Title change	None
1.7	October 2025	User Guide Template update.	Removed "Page Updated: Month Year" on each page. Changed CA-MMIS to California Medicaid Management Information System.
1.8	December 2025	Updated content and screen shots	None
1.9	March 2026	Update	Added My Account sections, New Affiliation requests, updated screenshots