



Medi-Cal Provider Portal User Guide: Provider Organization

Department of Health Care Services (DHCS)

CA-MMIS

V 1.5

September 2024

Provider Portal User Guide: Provider Organization

The purpose of the *Provider Portal User Guide: Provider Organization* is a comprehensive instructional document. It provides an overview of portal features, step-by-step instructions for how to use these features, and more.

Table of Contents

Introduction to the Provider Portal	1
Register an Organization	2
Add a User	9
Add a New Organization	19
Set Passkey	21
Provider Portal Overview.....	22
Dashboard.....	22
One-Time Passcode.....	24
Select an Organization	25
Add or Switch Organizations	26
Change a Password	27
Reset a Forgotten Password.....	29
Unlock Account/Reset Password	32
Going Paperless.....	33
Provider Portal Features.....	36
My Profile and Preferences	36
Edit Personal Information	36
Edit Phone Number	37
Edit Passkey	38
Edit NPI Preferences.....	40
Edit Tax Document Enrollment.....	40
Edit Notification Preferences	44
Transaction Center.....	46
Transaction Testing.....	48
Administration	54
Updating User Information/Permissions	55
Deactivate User.....	56

Provider Portal User Guide: Provider Organization

Reactivate User.....	59
Domain Management.....	61
Notifications.....	62
Submitter Management.....	63
New Affiliation Request to a Submitter Organization.....	64
Approve a Submitter Affiliation Request.....	67
Deny a Submitter Affiliation Request.....	72
Manage Submitters	73
Submitter Directory.....	79
NPI Agreements and Settings	80
PIN Management	80
835 Receiver Management	82
Transactions Available	89
Presumptive Eligibility Provider Agreements.....	91
Communication Center.....	91
Search Correspondence	92
View/Download New Correspondence	93
Run Recent Searches	94
View Provider Welcome Letters	94
Change Summary.....	96

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 communications between the Department of Health Care Services (DHCS) and provider communities, increasing the security and accessibility of Medi-Cal electronic services and empowering providers in managing their organization to support their billing needs. The Provider Portal allows providers and billers to:

- Perform billing work for multiple National Provider Identifiers (NPIs) with a single administrative account
- Interact with Medi-Cal more seamlessly
- Go Paperless
- Find correspondence easily in the Communication 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
- Use a single-sign-on to link directly to Transaction Services without an additional log in
- Perform self-service capabilities, such as password and NPI Provider Identification Number (PIN) reset
- Complete provider-submitter affiliations and submit Claims 837 and Eligibility Benefit 270/271 test transactions

Register an Organization

This is the first step in setting up the Provider Portal for an organization and should be completed by one trusted individual. This person will automatically be given the role of Administrator in the Provider Portal, including permissions for all NPIs and correspondence.

When registering an organization, DHCS will issue a one-time registration token directly to the designated individual. This token will be sent by hard-copy (paper) letter 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 an appropriate person has been selected as the Provider Portal Administrator, and has received the token, the steps below should be followed:

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

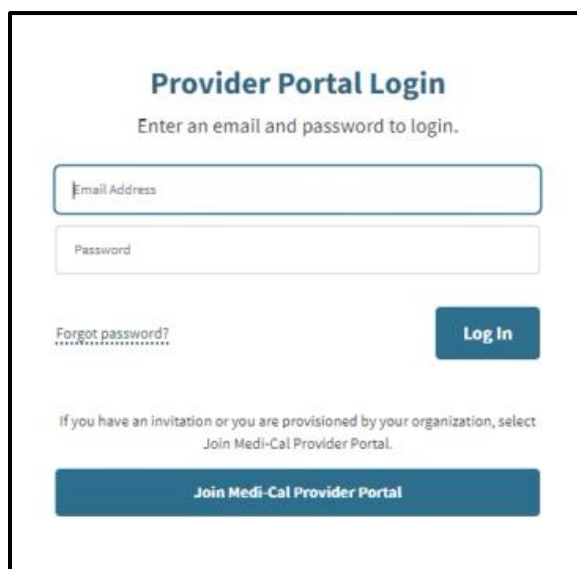


Figure 1.1: Join Medi-Cal Provider Portal Log In.

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

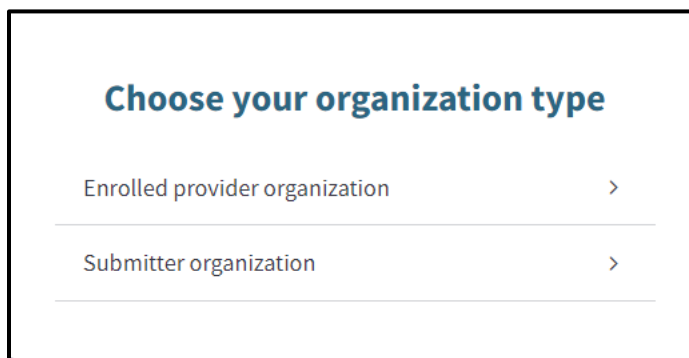
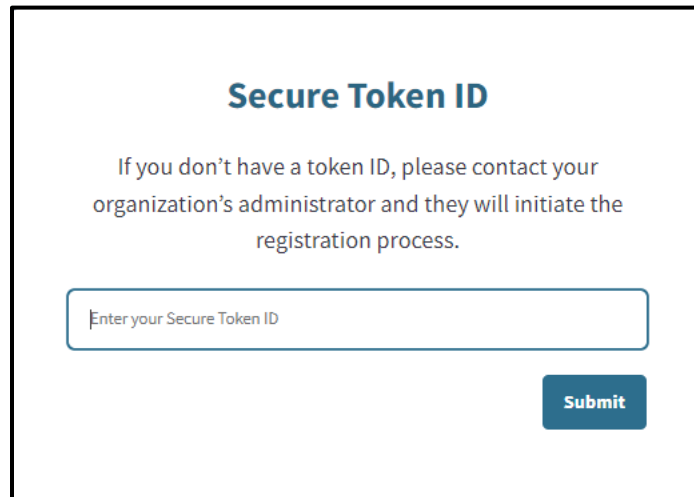


Figure 1.2: Choose your organization type.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

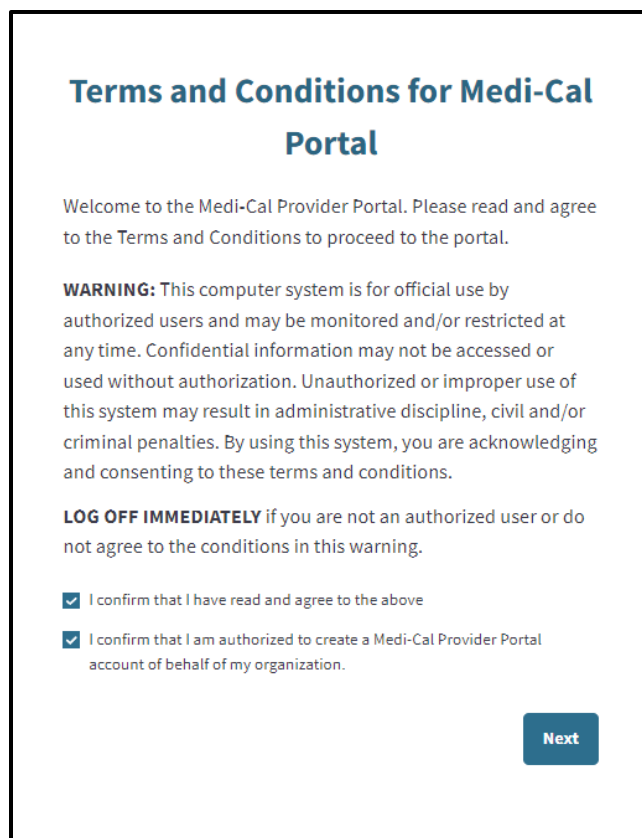
3. The **Secure Token ID** pop-up window appears.



The image shows a pop-up window titled "Secure Token ID". Below the title, there is a message: "If you don't have a token ID, please contact your organization's administrator and they will initiate the registration process." Below this message is a text input field with the placeholder text "Enter your Secure Token ID". To the right of the input field is a blue button labeled "Submit".

Figure 1.3: Secure Token ID.

4. Enter the unique token and select **Submit**. A **Terms and Conditions for the Medi-Cal Provider Portal** window displays.



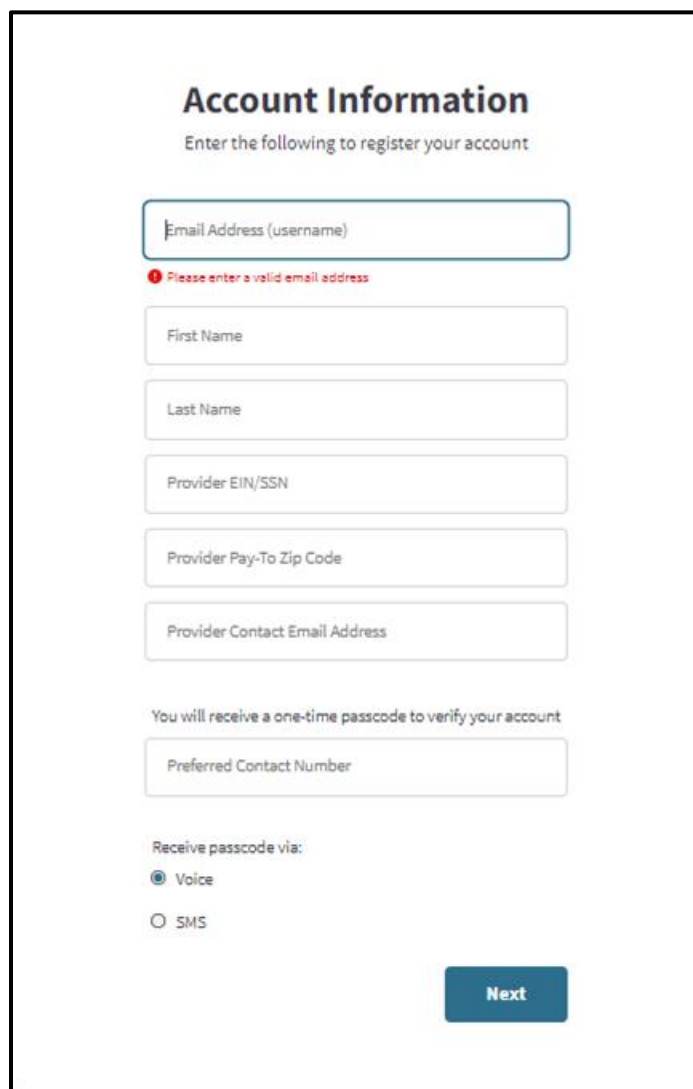
The image shows a window titled "Terms and Conditions for Medi-Cal Portal". Below the title, there is a welcome message: "Welcome to the Medi-Cal Provider Portal. Please read and agree to the Terms and Conditions to proceed to the portal." Below this is a **WARNING** section: "WARNING: This computer 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." Below the warning is a **LOG OFF IMMEDIATELY** section: "LOG OFF IMMEDIATELY if you are not an authorized user or do not agree to the conditions in this warning." Below this are two checkboxes, both of which are checked: "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." At the bottom right of the window is a blue button labeled "Next".

Figure 1.4: Terms and Conditions for Medi-Cal Portal.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

5. 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.” Click **Next** and the **Account Information** window appears.
6. Enter an **Email, First Name, Last Name, Provider Employer Identification Number/Social Security Number (EIN/SSN), Provider Pay-To ZIP** associated with the EIN/SSN, and **Provider Contact Email Address**.



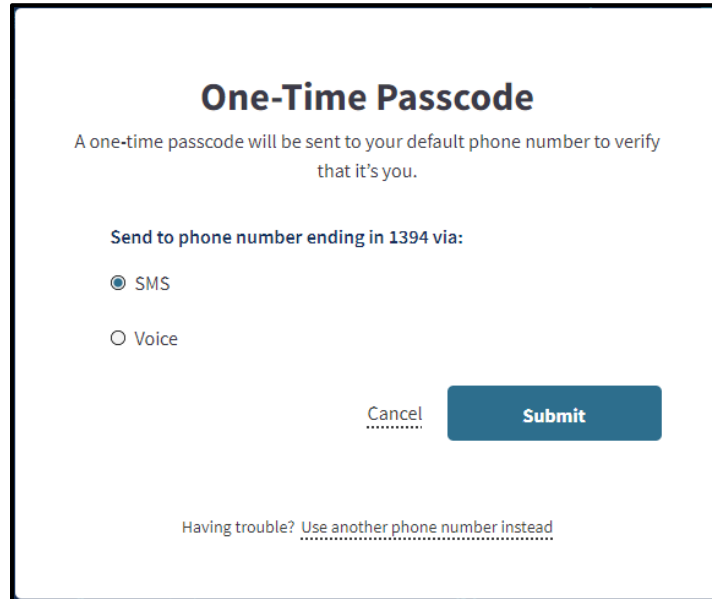
The screenshot shows a web form titled "Account Information" with the subtitle "Enter the following to register your account". The form contains several input fields: "Email Address (username)" (with a red error message "Please enter a valid email address"), "First Name", "Last Name", "Provider EIN/SSN", "Provider Pay-To Zip Code", and "Provider Contact Email Address". Below these fields is a section for "You will receive a one-time passcode to verify your account" with a "Preferred Contact Number" field. At the bottom, there are radio buttons for "Receive passcode via:" with options "Voice" (selected) and "SMS". A blue "Next" button is located at the bottom right of the form.

Figure 1.5: Account Information.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

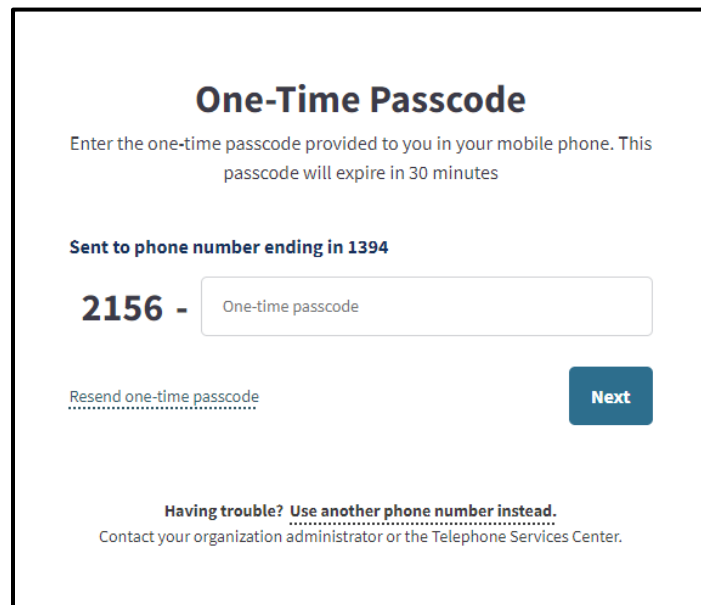
7. To verify the account, a One-Time Passcode (OTP) will be sent to the Administrator's phone. The Administrator will need to indicate how to receive this passcode, via SMS (text) or Voice (call). Select the method and click **Next**.



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, there are two buttons: "Cancel" and "Submit". Below the "Cancel" button, there is a link that says "Having trouble? Use another phone number instead".

Figure 1.6: One-Time Passcode.

8. A screen to enter the OTP appears. Enter the last six digits of the code that was sent to the phone and click **Next**.



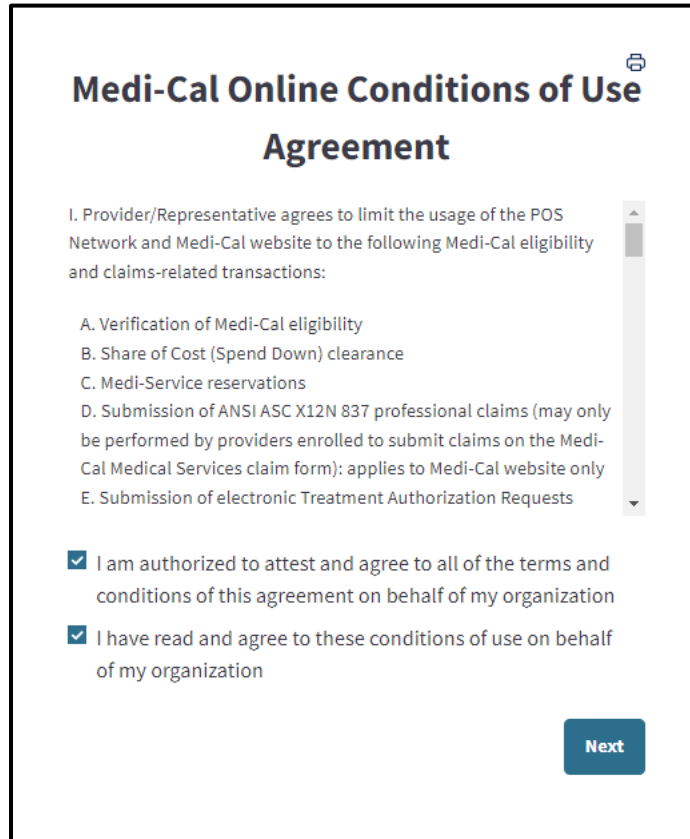
The screenshot shows a mobile application screen titled "One-Time Passcode". Below the title, it says "Enter the one-time passcode provided to you in your mobile phone. This passcode will expire in 30 minutes". There is a text input field with the placeholder "One-time passcode". To the left of the input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

Figure 1.8: Enter One-Time Passcode.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

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



The screenshot shows a web form titled "Medi-Cal Online Conditions of Use Agreement" with a printer icon in the top right corner. The form contains a list of conditions (I through E) and two checkboxes for agreement. 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 1.9: Medi-Cal Online Conditions of Use Agreement.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

10. A window appears stating, "Registration Complete." An email will be sent to the email indicated during sign-up, to set up a password. Select the link to continue the registration process. **This must be done within 10 minutes, or the link will expire.** If this process is not completed within 10 minutes, the Administrator may initiate a password reset with the email used during registration in order to gain access to the portal.

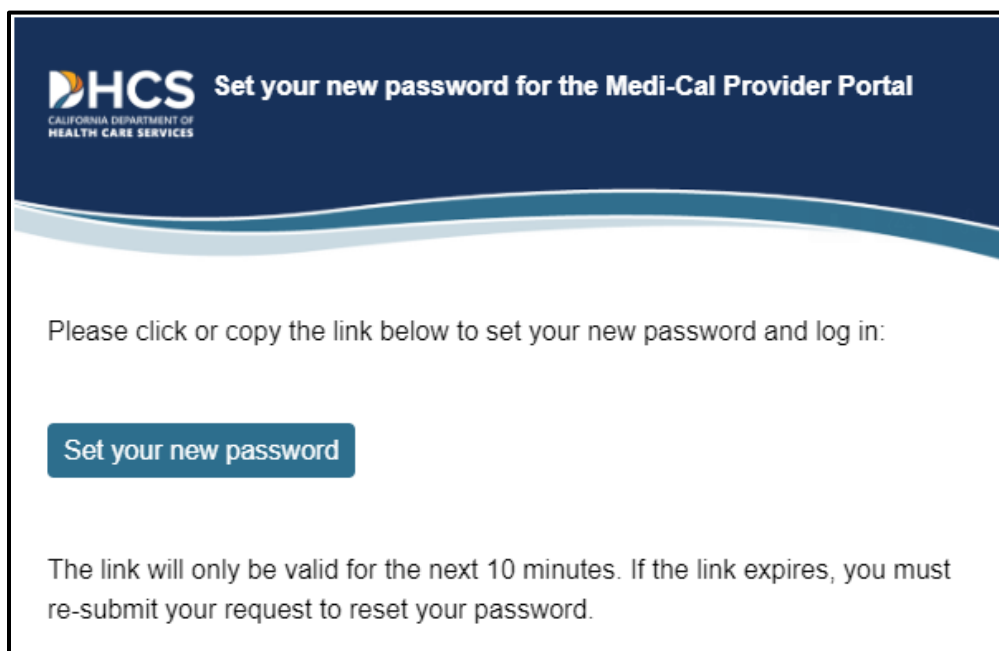
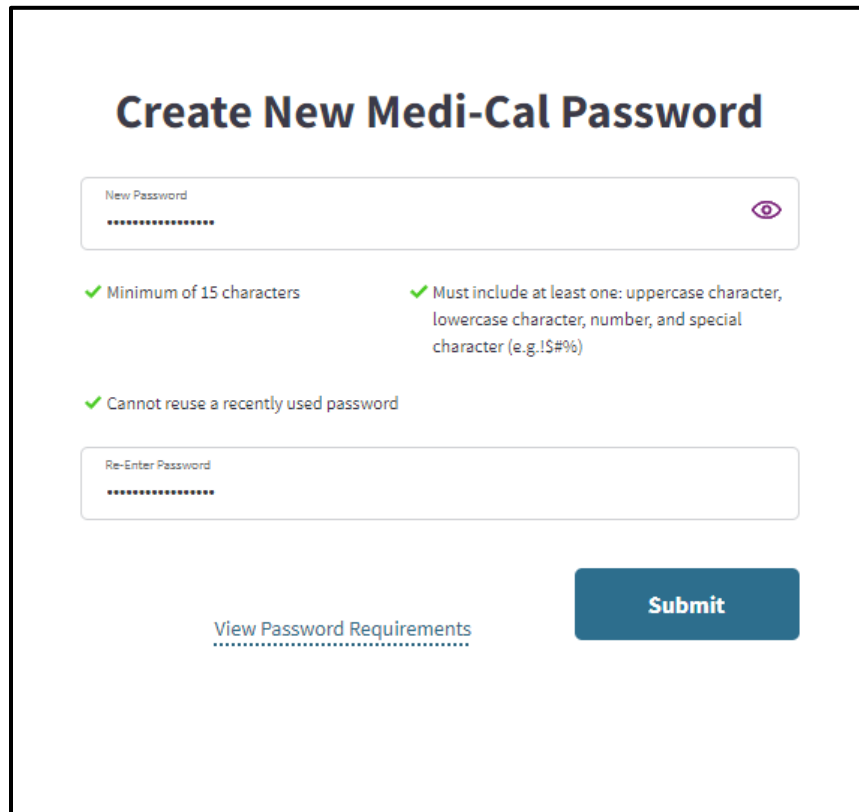


Figure 1.10: Set new password email notification.

11. A pop-up window to create a new password will appear. Enter a password that aligns with the password criteria and click **Submit**.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

The screenshot shows a web form titled "Create New Medi-Cal Password". It features two input fields: "New Password" and "Re-Enter Password", both masked with asterisks. To the right of the "New Password" field is an eye icon for toggling visibility. Below the input fields are three green checkmark icons indicating password requirements: "Minimum of 15 characters", "Must include at least one: uppercase character, lowercase character, number, and special character (e.g. !\$#%)", and "Cannot reuse a recently used password". At the bottom, there is a link "View Password Requirements" and a blue "Submit" button.

Create New Medi-Cal Password

New Password

✓ Minimum of 15 characters

✓ Must include at least one: uppercase character, lowercase character, number, and special character (e.g. !\$#%)

✓ Cannot reuse a recently used password

Re-Enter Password

[View Password Requirements](#)

Submit

Figure 1.11: Create New Medi-Cal Password.

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.

12. The Administrator has now successfully registered the organization and has administrative privileges to all NPIs in the organization.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

Add a User

An Administrator can complete the following steps to add a new user:

1. From the Administration tile, select **Add a User**. The **Add a User** window appears to enter user information.

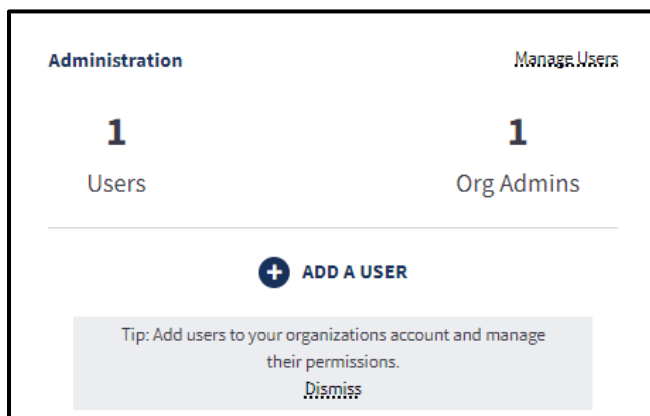


Figure 1.12: Administration Tile.

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

A screenshot of the 'Add a user to your organization' form. The form has a title 'Add a user to your organization' at the top. Below the title, there is a section labeled 'ORGANIZ' with five input fields: 'Email Address', 'First Name', 'Last Name', 'Mobile Number', and 'Business Number'. At the bottom right, there are two buttons: 'Cancel' and 'Next'.

Figure 1.13: 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 following steps 4 through 11 apply to the new user who was added. **The Administrator may skip to step 12 to set up a user's permissions.**

Provider Portal User Guide: Provider Organization

Page updated: March 2024

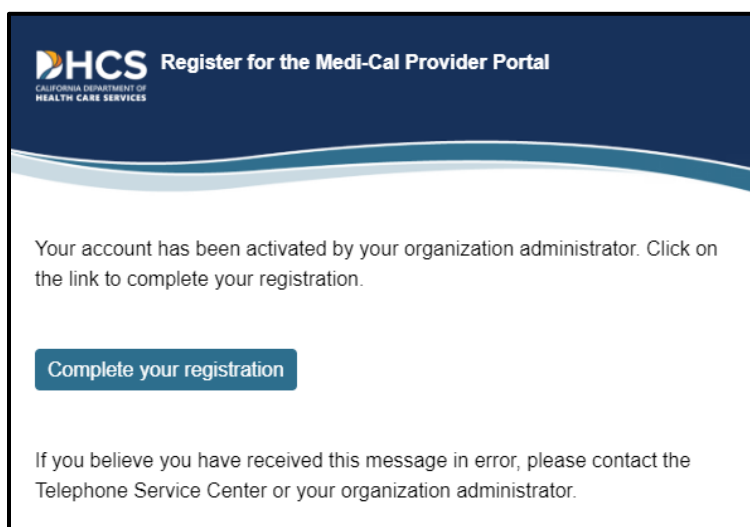


Figure 1.14: Register for the Medi-Cal Provider Portal email notification.

4. The added user clicks the link provided in the registration email. A **Terms and Conditions for Medi-Cal Portal** window displays.

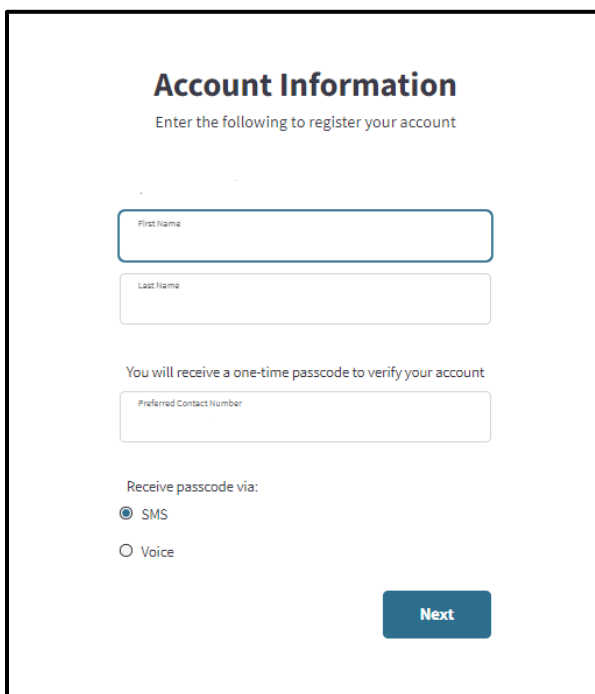
The image is a screenshot of a web window titled 'Terms and Conditions for Medi-Cal Portal'. The title is in blue. The main text is in black and reads: 'Welcome to the Medi-Cal Provider Portal. Please read and agree to the Terms and Conditions to proceed to the portal.' Below this is a 'WARNING' section in bold, followed by a paragraph of text. Then, there is a 'LOG OFF IMMEDIATELY' section in bold, followed by a paragraph of text. At the bottom, there is a checkbox with a blue checkmark and the text 'I confirm that I have read and agree to the above'. To the right of the checkbox is a blue button with the text 'Next'.

Figure 1.15: Terms and Conditions for Medi-Cal Portal.

5. The user reads the terms and conditions and selects **I confirm that I have read and agree to the above** and clicks **Next**. The **Account Information** window appears.
6. The user enters her **First Name**, **Last Name** and **Preferred Contact Number**.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

A registration form titled "Account Information" with the instruction "Enter the following to register your account". It contains input fields for "First Name", "Last Name", and "Preferred Contact Number". Below these is a section "Receive passcode via:" with radio buttons for "SMS" (selected) and "Voice". A blue "Next" button is at the bottom right.

Account Information

Enter the following to register your account

First Name

Last Name

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

Preferred Contact Number

Receive passcode via:

☒ SMS

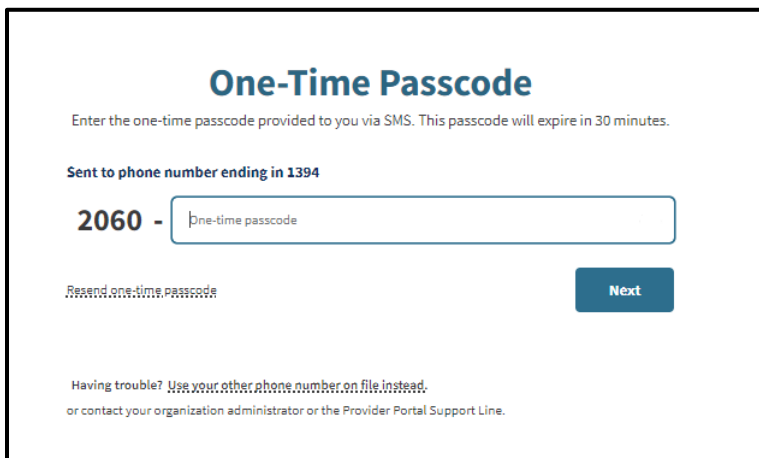
☐ Voice

Next

Figure 1.16: Account Information.

7. To verify the account, an OTP will be sent to the user's phone. The user will need to indicate how to receive this passcode, via SMS (text) or Voice (call). Select the method and click **Next**.
8. A screen to enter an OTP appears for the user. The user enters the last six digits of the code that was sent to the phone and clicks **Next**.

Note: Depending on the user's phone carrier, there may be a delay in receiving an OTP. The user should wait for the OTP to be received. If 10 minutes has passed and the user has not received an OTP, they may click **Resend one-time password**.

A screen titled "One-Time Passcode" with the instruction "Enter the one-time passcode provided to you via SMS. This passcode will expire in 30 minutes." It shows "Sent to phone number ending in 1394" and "2060 -" followed by an input field for the "one-time passcode". A link "Resend one-time password" is on the left, and a blue "Next" button is on the right. At the bottom, it says "Having trouble? Use your other phone number on file instead. or contact your organization administrator or the Provider Portal Support Line.".

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 - one-time passcode

Resend one-time password

Next

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

Figure 1.17: Enter One-Time Passcode.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

9. A window appears stating, “Registration Complete.”

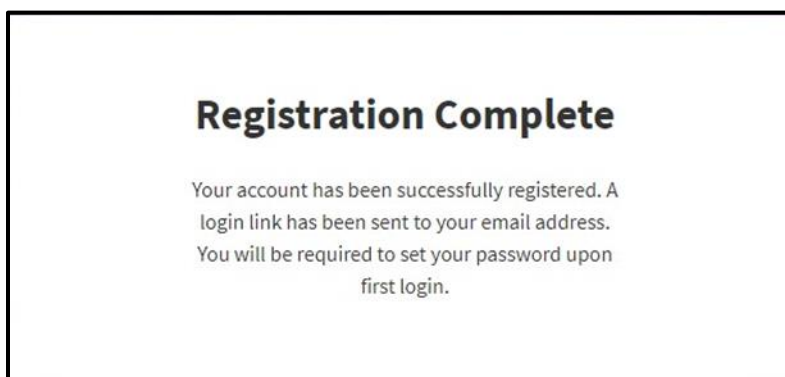


Figure 1.18: Registration Complete.

10. An email will be sent to the user's registered email address to set up a password. The user must select the link in the email **within 10 minutes or it will expire.**

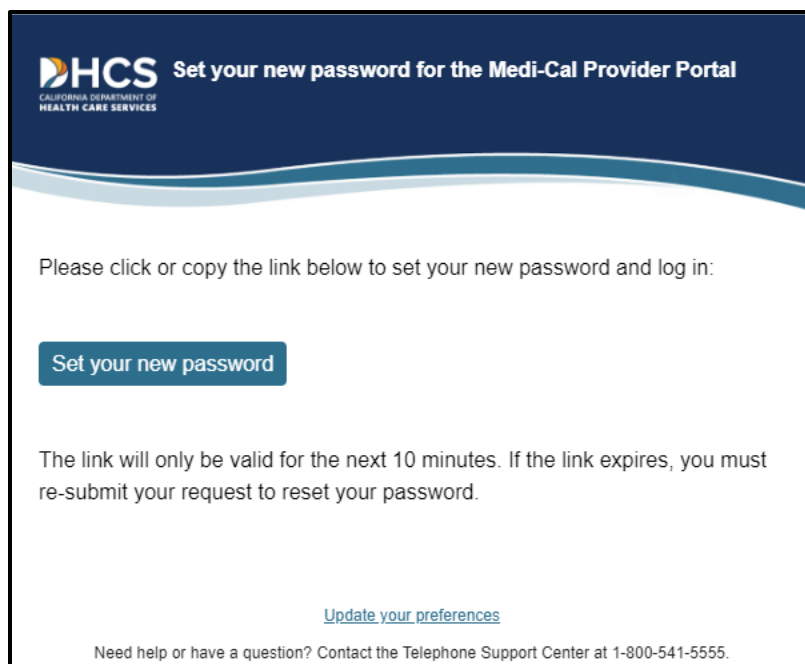


Figure 1.19: Set new password email notification.

11. A pop-up window to create a new password will appear. Enter a password that aligns with the password criteria and click **Submit**.

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.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

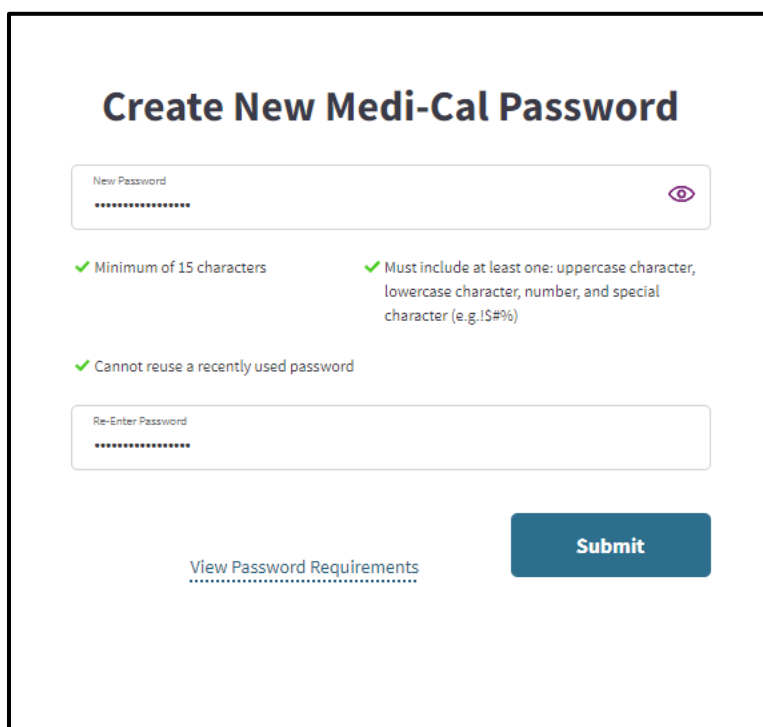
The screenshot shows a web form titled "Create New Medi-Cal Password". It features two input fields: "New Password" and "Re-Enter Password", both masked with dots. To the right of the "New Password" field is an eye icon for toggling visibility. Below the "New Password" field, there are three green checkmarks indicating password requirements: "Minimum of 15 characters", "Must include at least one: uppercase character, lowercase character, number, and special character (e.g. !\$#%)", and "Cannot reuse a recently used password". Below the "Re-Enter Password" field, there is a link "View Password Requirements" and a blue "Submit" button.

Figure 1.20: Create New Medi-Cal Password.

12. The new user is now successfully registered and may log into the account at any time.
13. To continue setting up the new user's permissions: The Administrator may select **Skip For Now** to assign permissions at a later time or **Assign Now**. 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 (refer to the "Update User Information/Permissions" section). If the option **Assign Now** is selected, refer to the following steps.

Note: If permissions are never assigned, eventually the user will be deactivated, and the Administrator will need to reactivate the user.

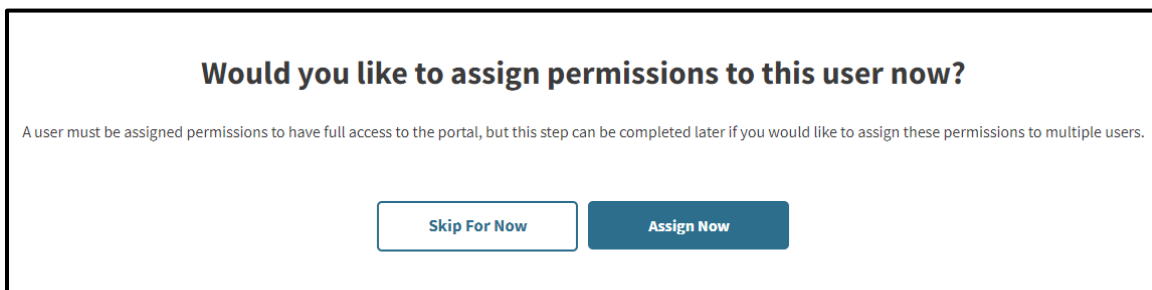
The screenshot shows a dialog box with the title "Would you like to assign permissions to this user now?". Below the title is a note: "A user must be assigned permissions to have full access to the portal, but this step can be completed later if you would like to assign these permissions to multiple users." At the bottom of the dialog are two buttons: "Skip For Now" and "Assign Now".

Figure 1.21: Assign User Permissions.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

14. The **Assign NPI Permissions** page appears. **Step 1: Assign NPI Permissions** is required. Select one of the following level of permissions for each NPI:

- **Administrator:** Users with an NPI role of administrator will have access to view and reset NPI PINs and view tax documents and correspondence that has 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.

Email:
Mobile Phone:
Business Phone:

Step 1

Assign NPI Permissions (Required)

Assign this user to NPIs within this organization, and select permission levels. If the user is an organization admin, they have automatically been given full permissions to all NPIs. All NPIs do not have to be assigned.

Q Search Quick Assign to All NPIs

All (1) Assigned (0) Unassigned (1)

NPI	Legal Name	Status	Permissions
		Unassigned	<input type="checkbox"/> Admin <input type="checkbox"/> Processor <input checked="" type="checkbox"/> None

Cancel Update

Figure 1.22: Assign NPI Permissions.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

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.

Email:
Mobile Phone:
Business Phone:

Step 1

Assign NPI Permissions (Required)

Assign this user to NPIs within this organization, and select permission levels. If the user is an organization admin, they have automatically been given full permissions to all NPIs. All NPIs do not have to be assigned.

Q Search

Quick Assign to All NPIs

Admin

Processor

None

All (1) Assigned (0) Unassigned (1)

NPI	Legal Name	Status	Permissions
		Unassigned	<input type="checkbox"/> Admin <input type="checkbox"/> Processor <input checked="" type="checkbox"/> None

Cancel Update

Figure 1.23: Step 1 Quick Assign to All NPIs.

15. Once the Administrator has completed assigning the user's NPI Permissions, click **Next**.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

16. The **Step 2: Assign Correspondence Permissions** page appears. This step is optional and may be updated later. Correspondence for NPIs only appear in this area if the user is assigned to the NPI.

To assign permissions, select the correspondence permissions to assign and click **Manage Selected** in the top right corner, or click **Manage** next to the NPI to assign permissions for a single NPI.

Step 1

Edit

Assign NPI Permissions (Required)

Complete

Step 2

Assign Correspondence Permissions (Optional)

Assign this user permissions to view and download selected correspondence types within their assigned NPIs. Users must be assigned to an NPI to have access to correspondence.

Search

Filter

Manage Selected

All (1)

Correspondence Permissions Assigned (0)

Unassigned (1)

Select All

NPI

Legal Name

Correspondence Permissions

None

Manage

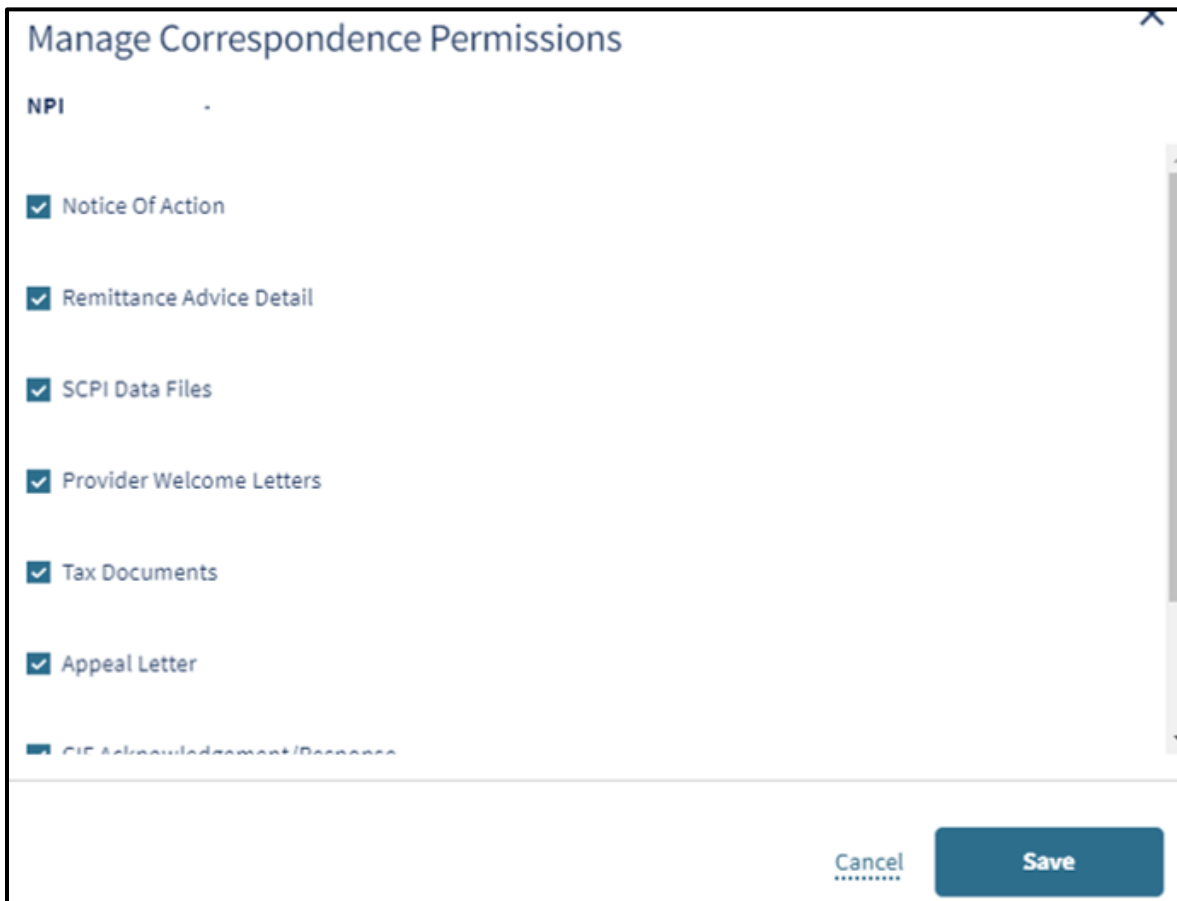
Next

Figure 1.24: Step 2 Assign Correspondence Permissions.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

17. The **Manage Correspondence Permissions** window appears. Select the applicable correspondence type(s) and click **Save**.



Manage Correspondence Permissions

NPI -

- ☒ Notice Of Action
- ☒ Remittance Advice Detail
- ☒ SCPI Data Files
- ☒ Provider Welcome Letters
- ☒ Tax Documents
- ☒ Appeal Letter
- ☒ CIE Acknowledgment/Response

Cancel Save

Figure 1.25: Manage Correspondence Permissions.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

18. Once the Administrator has completed adding correspondence permissions, click **Next**.
19. The **Step 3: Assign Permissions Across Organization** window appears for the Administrator to assign organization-level user permissions to add, remove or modify users. This step is optional and may be updated later. Click the dropdown menu and choose **Administrator**, **Processor** or **None**. Click **Save and Finish**.

Step 1 Edit

Assign NPI Permissions (Required)

✓ Complete

Step 2 Edit

Assign Correspondence Permissions (Optional)

✓ Complete

Step 3

Assign Permissions Across Organization (Optional)

Assign an organization permission level to this user.

None ▲

Admin

Processor

✓ None

Administrator 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. However, this administrator will NOT automatically be assigned correspondence permissions. If this administrator needs to access correspondence, you will need to manually assign correspondence permissions above. Assign this role with care.

None will give the user no permissions at an organization level. NPI level permissions can still be set. Most users will fall into this permission level.

Save

Figure 1.26: Step 3 Assign Permissions Across Organization.

20. A confirmation page appears containing the new user's information as entered. If any information is incorrect, click **Edit** next to the incorrect field.

Add a New Organization

An Administrator can complete the following steps to add a new organization:

1. Log in to the Provider Portal and click the **Add or Switch Organization** drop-down menu, then click **Add a New Organization**.

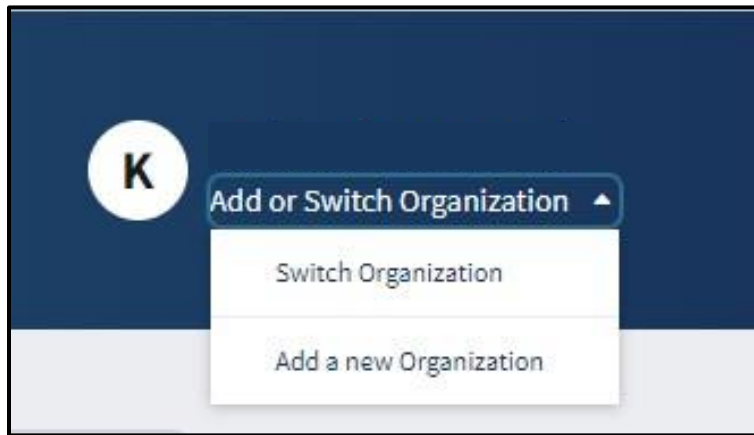


Figure 1.27: Add or Switch Organization.

2. Enter the **Secure Token ID** from the token letter.

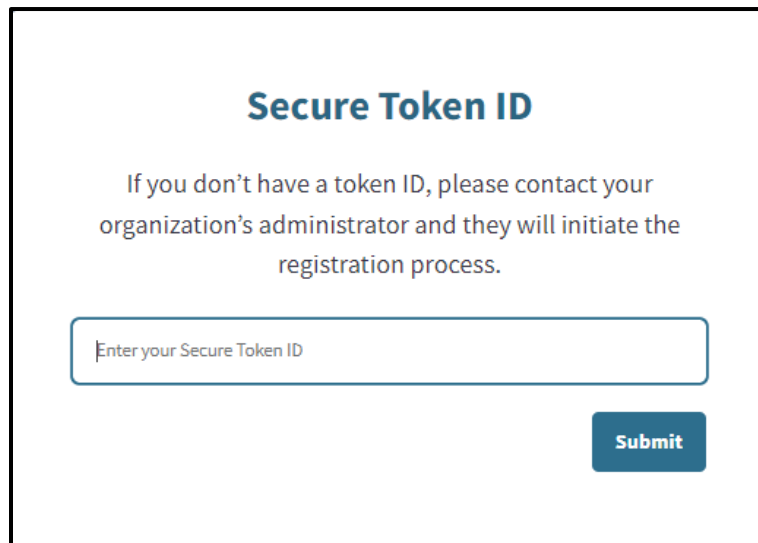
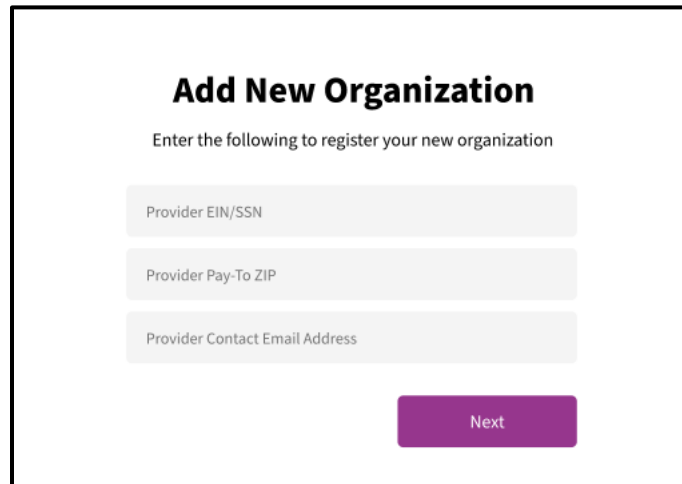
A screenshot of a form titled 'Secure Token ID' in bold blue text. Below the title is a paragraph: 'If you don't have a token ID, please contact your organization's administrator and they will initiate the registration process.' Below this is a text input field with the placeholder text 'Enter your Secure Token ID'. To the right of the input field is a blue 'Submit' button.

Figure 1.28: Secure Token ID.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

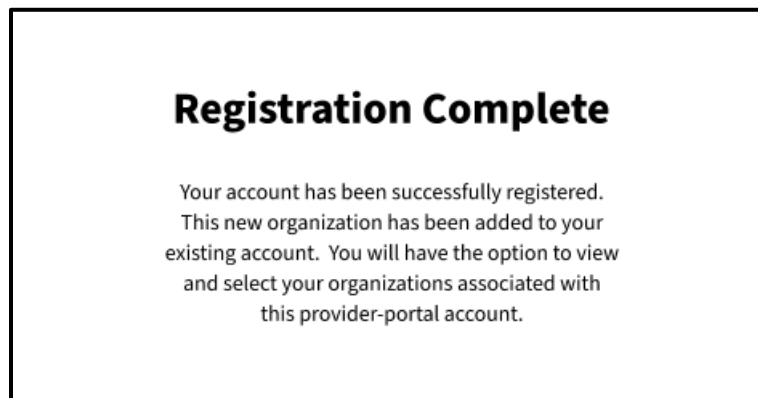
3. Enter the **Provider EIN/SSN**, **Provider Pay-To ZIP** associated with the EIN/SSN, and **Provider Contact Email Address**. Click **Next**.



The screenshot shows a web form titled "Add New Organization". Below the title is a subtitle: "Enter the following to register your new organization". There are three input fields, each with a light gray border and placeholder text: "Provider EIN/SSN", "Provider Pay-To ZIP", and "Provider Contact Email Address". At the bottom right of the form is a purple button with the text "Next".

Figure 1.29: Add New Organization.

4. Registration is complete. In order to view the new organization, log out of the Provider Portal and log back in.



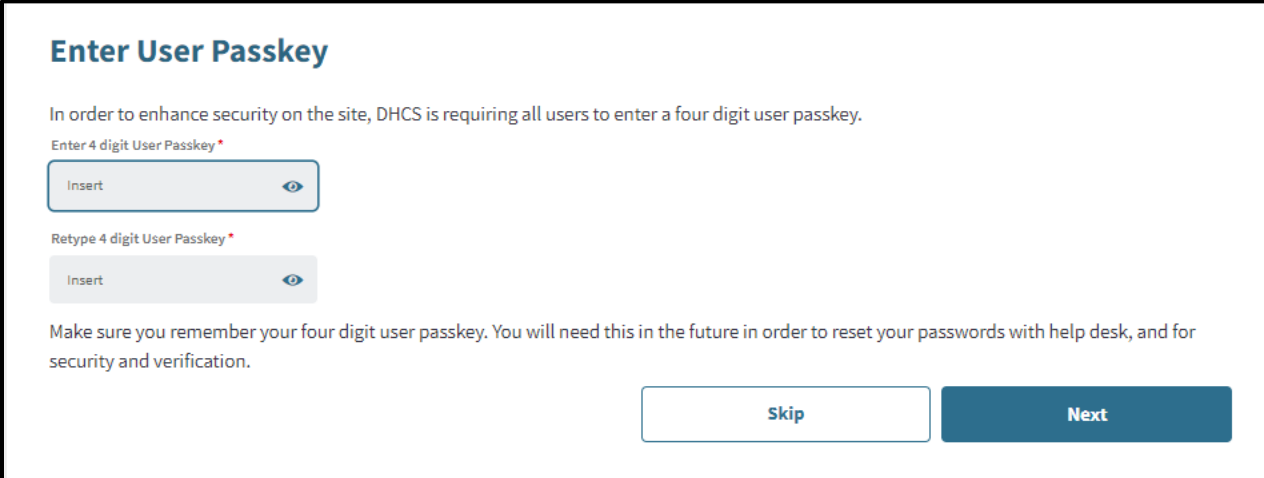
The screenshot shows a confirmation message titled "Registration Complete". The text below the title reads: "Your account has been successfully registered. This new organization has been added to your existing account. You will have the option to view and select your organizations associated with this provider-portal account."

Figure 1.30: Registration Complete.

Set Passkey

After registration is complete, the **Enter User Passkey** screen will appear to create a four (4) digit passkey for additional security. Once the new passkey is entered, click **Next** to continue or click **Skip** to bypass adding the new passkey.


Note: The passkey can be set later from the **My Profile and Preference** tile 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 1.31: Enter User Passkey.

Provider Portal User Guide: Provider Organization

Page updated: May 2024

Provider Portal Overview

The Provider Portal is designed to house communications, notifications and organization information. Users within a provider organization have the option to be assigned as an Administrator or a Processor.

The **Administrator** will have access to all Provider Portal features and organization administration functions. The **Processor** will be able to make use of the organization features, such as Transaction Testing and access to the Transaction Center but will not have access to the organization administration functions.

Dashboard

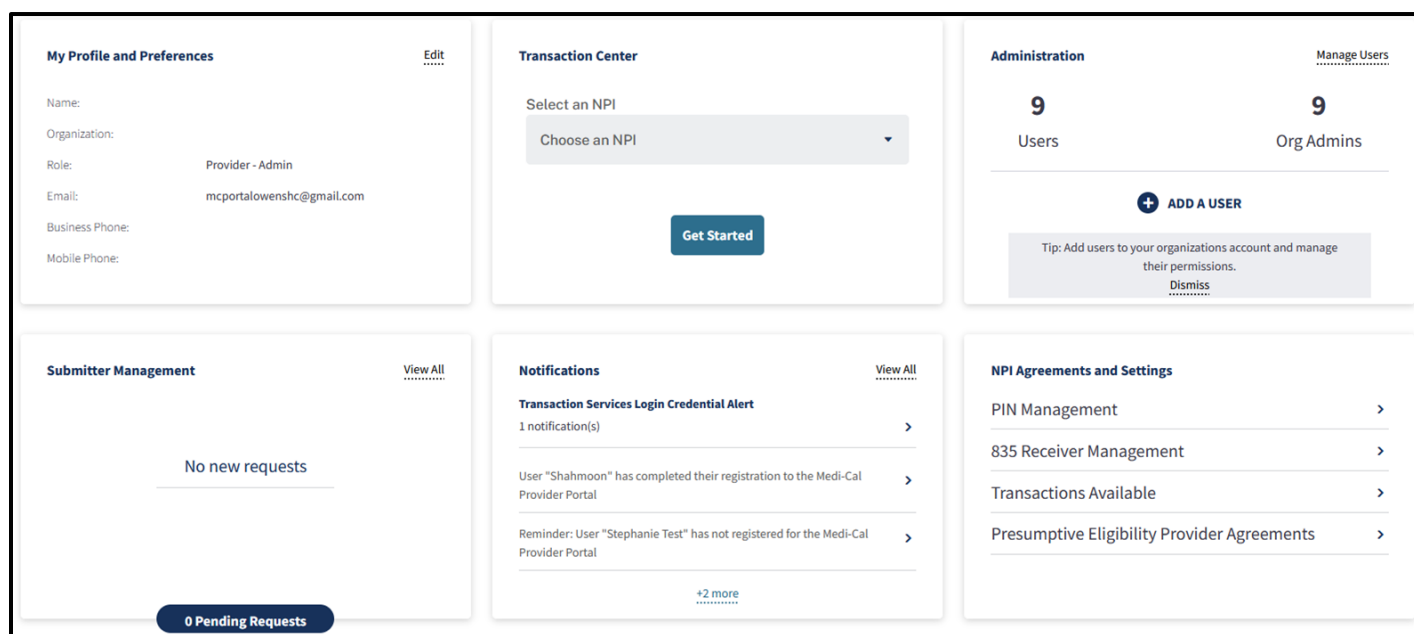


Figure 1.32: Provider Admin Dashboard.

The portal contains seven (7) areas on the **Dashboard**. Detailed information about each can be found later in this user guide. Here is an overview:

1. **My Profile and Preferences** contains user contact information and allows adjustment to email notification settings.
2. The **Transactions Center** allows users to create and keep track of various transactions, and single sign on to Transaction Services.

Provider Portal User Guide: Provider Organization

Page updated: May 2024

3. **Administration** displays information about users within an organization. This area permits Administrators to: update user permissions and information, to add and/or remove user profiles.
4. **Submitter Management** allows a user to view new affiliation and pending requests, manage submitters and view the submitter directory.
5. **Notifications** allows a user to view unread and past notifications about an organization. Notifications can be searched for or filtered by date.
6. **NPI Agreements and Settings** allows a user to search for NPIs within an organization, update NPI Provider Identification Numbers (PINs), manage 835 receivers, Transactions Available and Presumptive Eligibility Provider Agreements.
7. **Communication Center** allows a user to electronically search, view and download correspondence related to the organization.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

One-Time Passcode

The Provider Portal uses two-factor authentication to ensure security. At any time while conducting business in the Portal, a page prompting the user to enter an OTP may appear.

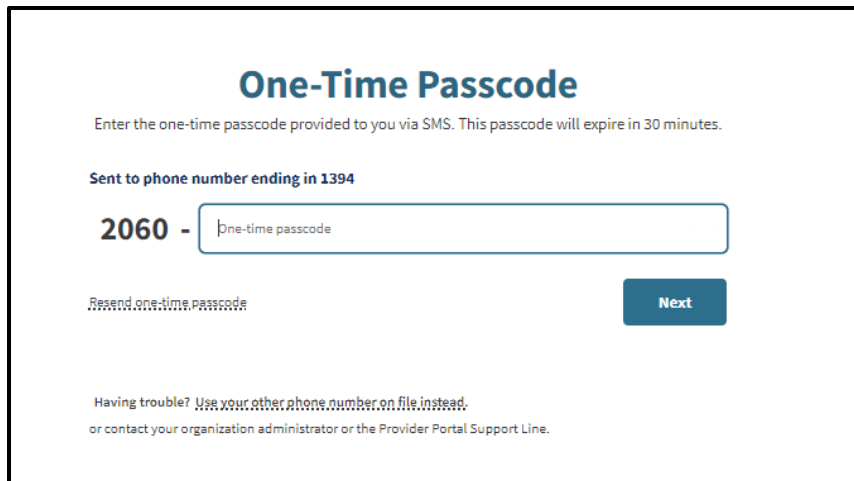
The screenshot shows a web form titled "One-Time Passcode" in a blue header. Below the title, a message states: "Enter the one-time passcode provided to you via SMS. This passcode will expire in 30 minutes." Underneath, it says "Sent to phone number ending in 1394". The main input area shows "2060 -" followed by a text box containing "One-time passcode". To the left of the text box is a small icon of a phone. Below the input area, there is a link "Resend one-time passcode" and a blue button labeled "Next". At the bottom, a footer note reads: "Having trouble? Use your other phone number on file instead, or contact your organization administrator or the Provider Portal Support Line."

Figure 1.33: One-Time Passcode.

If the page appears, a code is automatically sent to the user's phone, either via short message service (SMS) (text) or Voice (call) depending on how the user configured the settings. Enter the passcode and click **Next** to continue conducting business in the Portal.

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

Select an Organization

Upon first login, a screen appears prompting 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.)

This page 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.



Figure 1.34: Select an Organization.

From here, the user may select any organization available to them. This serves as the user's default organization.

Add or Switch Organizations

This feature is only available if a user has been granted access to multiple organizations by the organization's respective Administrator.

1. If a user wishes to switch to a different organization, the user can do so at any time by clicking the **Add or Switch Organization** drop-down menu from the **Dashboard**, then selecting **Switch Organization**.

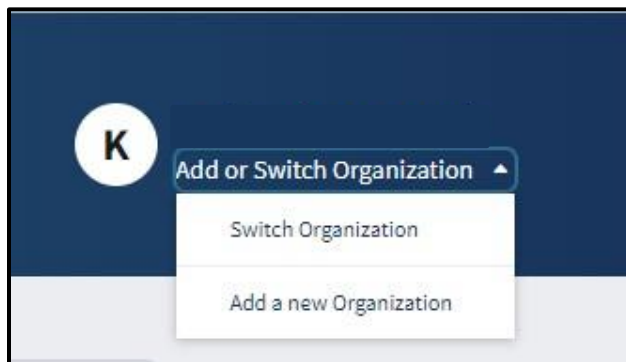


Figure 1.35: Add or Switch Organization.

2. The **Select an Organization** page appears and the user can add or switch organizations by selecting one of the items on the list.

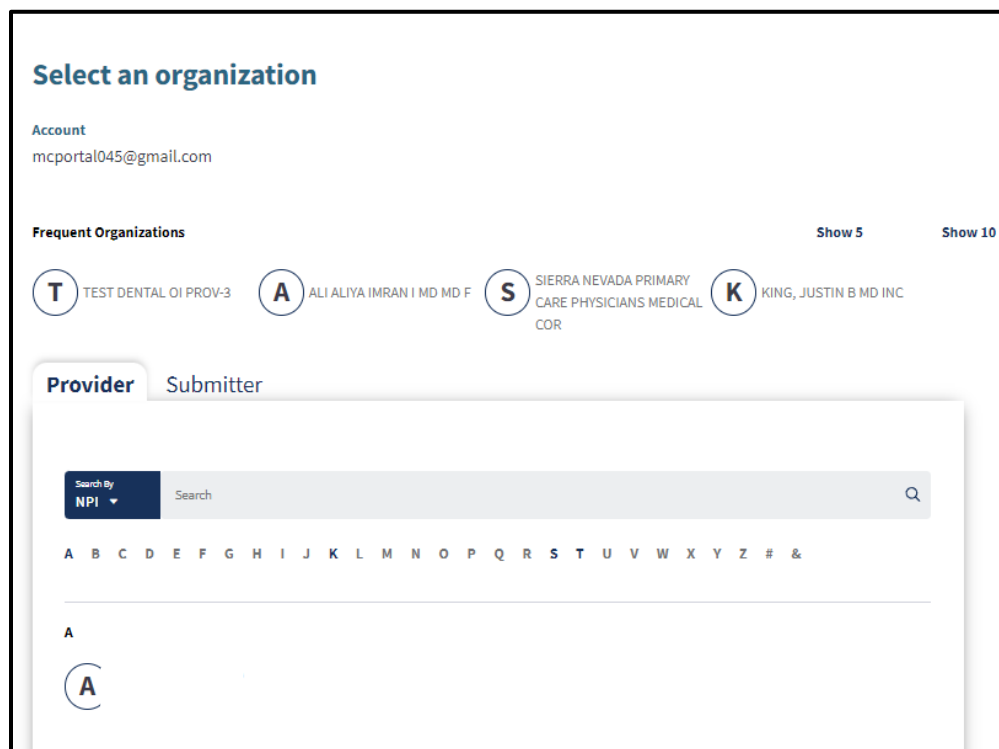
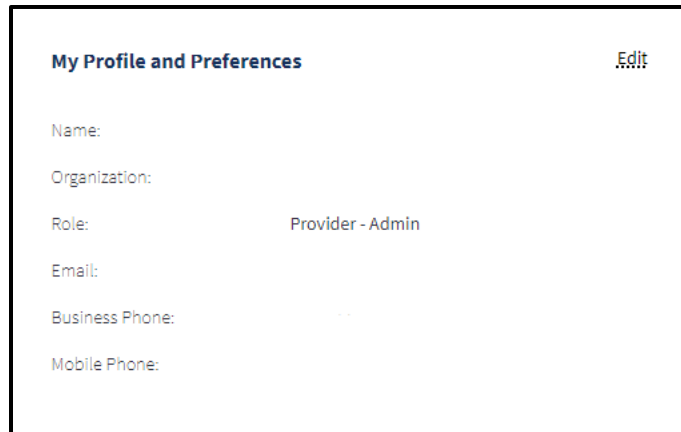


Figure 1.36: Select an Organization.

Change a Password

Users may change their own passwords:

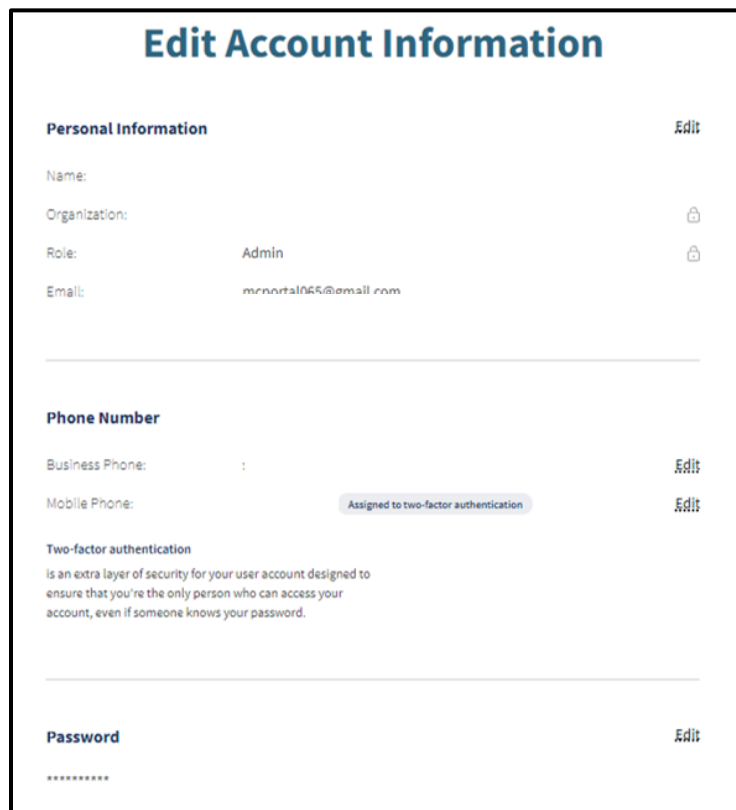
1. From **My Profile and Preferences** on the **Dashboard**, select **Edit**.



The screenshot shows a form titled "My Profile and Preferences" with an "Edit" link in the top right corner. The form contains several input fields: "Name:", "Organization:", "Role:" (with the value "Provider - Admin" displayed), "Email:", "Business Phone:", and "Mobile Phone:". The form is enclosed in a black border.

Figure 1.37: My Profile and Preferences.

2. A page to **Edit Account Information** appears. Scroll down to Password and click **Edit**.



The screenshot shows a page titled "Edit Account Information". It has three main sections: "Personal Information", "Phone Number", and "Password". Each section has an "Edit" link. The "Personal Information" section includes fields for "Name:", "Organization:", "Role:" (with the value "Admin" and a lock icon), and "Email:" (with the value "mrrnortal065@email.com"). The "Phone Number" section includes fields for "Business Phone:" and "Mobile Phone:" (with a value "Assigned to two-factor authentication" and a lock icon). The "Password" section has a field for the password (with a value "*****") and an "Edit" link. The page is enclosed in a black border.

Figure 1.38: Edit Account Information.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

3. An area to edit the account password appears. Enter the current password and a new password that follows the password guidelines.

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.

Re-enter the new password and select **Change Password**.

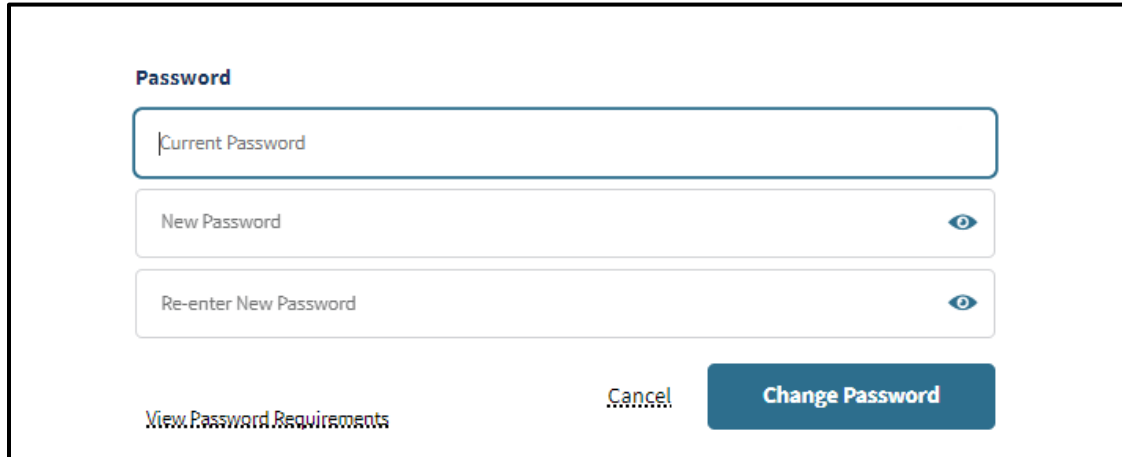
The screenshot shows a 'Change Password' form within a light gray border. At the top, the word 'Password' is written in blue. Below it are three input fields: 'Current Password', 'New Password', and 'Re-enter New Password'. The 'New Password' and 'Re-enter New Password' fields have a blue eye icon to their right, indicating a toggle for password visibility. At the bottom left is a link 'View Password Requirements' in blue. At the bottom center is a 'Cancel' link in blue. At the bottom right is a solid blue button with the text 'Change Password' in white.

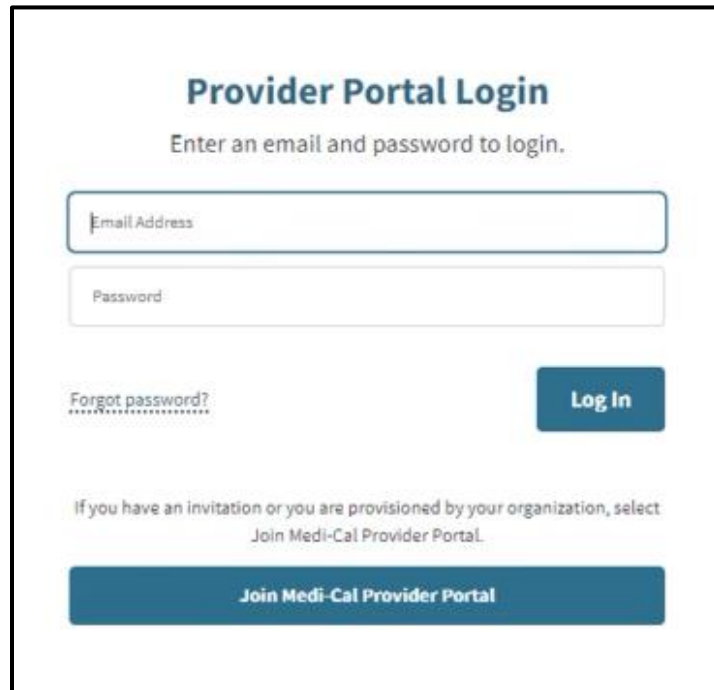
Figure 1.39: Change Password.

4. A confirmation screen appears, and the password is now updated.

Reset a Forgotten Password

If the user forgets the password and needs to reset it, the user may reset it by doing the following:

1. From the Log In screen, click **Forgot password.**



The screenshot shows the 'Provider Portal Login' interface. At the top, the title 'Provider Portal Login' is displayed in a bold, dark blue font. Below the title, a subtitle reads 'Enter an email and password to login.' in a smaller, grey font. The main form consists of two input fields: 'Email Address' and 'Password', both with light blue borders. To the right of the 'Password' field is a blue button labeled 'Log In'. Below the input fields, there is a link that says 'Forgot password?' with a series of dots underneath it. At the bottom of the form, there is a blue button labeled 'Join Medi-Cal Provider Portal'.

Figure 1.40: Medi-Cal Provider Portal Log In.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

2. From the window that appears, enter the appropriate email address, and click **Reset Password**.

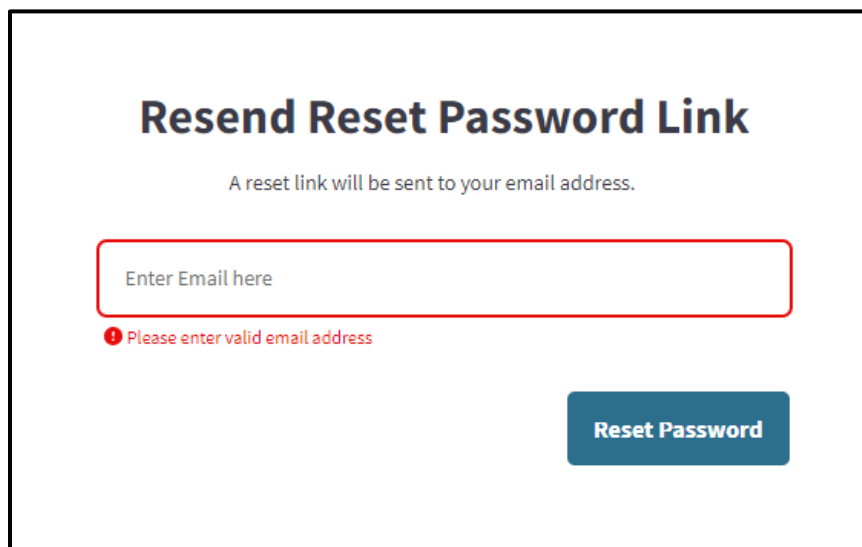
A screenshot of a web form titled "Resend Reset Password Link". Below the title is a sub-header: "A reset link will be sent to your email address." There is a text input field with the placeholder text "Enter Email here". Below the input field is a red error message: "Please enter valid email address". To the right of the input field is a blue button labeled "Reset Password".

Figure 1.41: Resend Reset Password Link.

3. A link to reset the password will be sent via email.

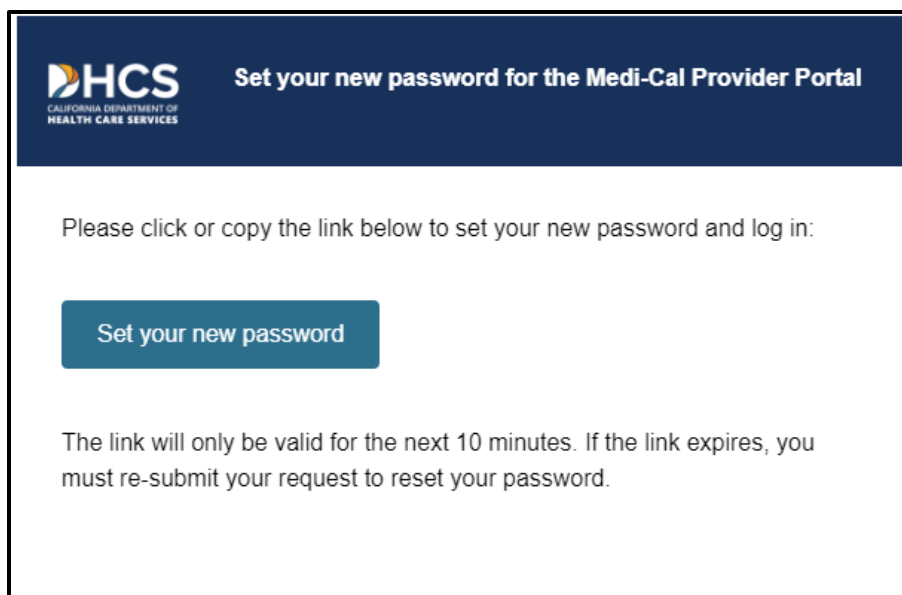
A screenshot of an email notification from the California Department of Health Care Services (DHCS). The header is dark blue with the DHCS logo and the text "Set your new password for the Medi-Cal Provider Portal". The main body of the email is white and contains the text: "Please click or copy the link below to set your new password and log in:". Below this text is a blue button labeled "Set your new password". At the bottom, it states: "The link will only be valid for the next 10 minutes. If the link expires, you must re-submit your request to reset your password."

Figure 1.42: Set new password email notification.

4. Click the link to reset the password. The user will be prompted to enter the last six digits of the passcode sent to their phone. Enter the code and click **Next**.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

Figure 1.43: Enter One-Time Passcode.

5. The **Create New Medi-Cal Password** page displays and the user can enter a new password and click **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.

Figure 1.44: Create New Medi-Cal Password.

Provider Portal User Guide: Provider Organization

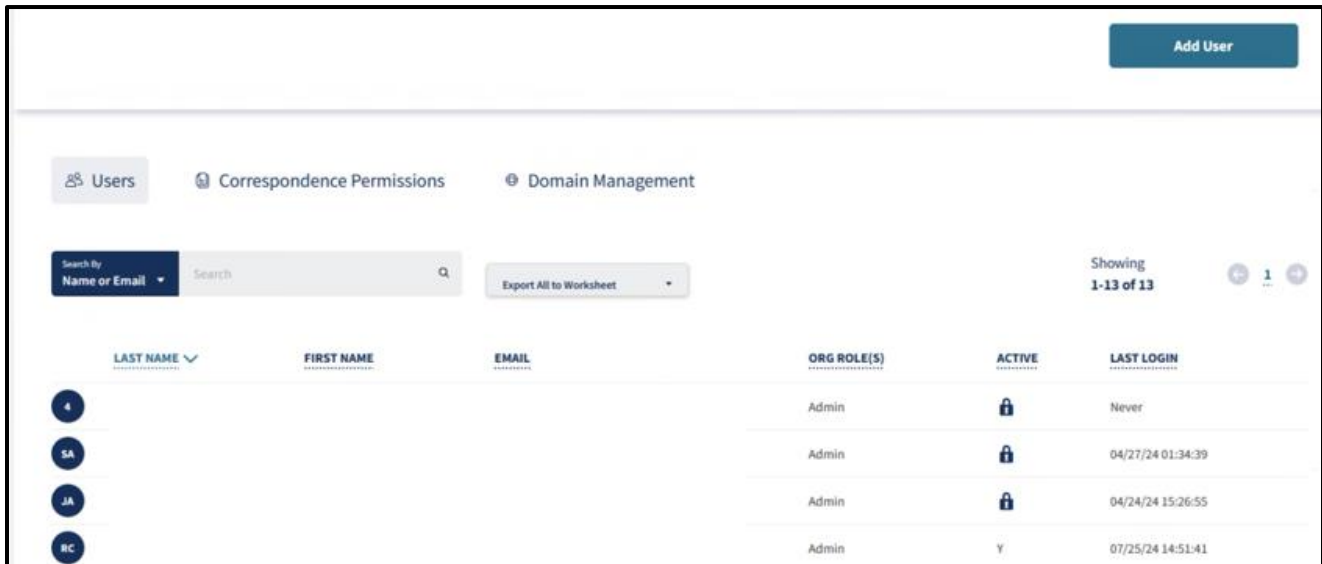
Page updated: September 2024

Unlock Account/Reset Password

A user account will become locked if it is inactive for more than 180 days. Passwords will remain locked until the password reset email is received and the password is updated.

To unlock an account, Administrators must follow these steps:

1. Within **User Management**, the accounts that are locked have the lock symbol (🔒) in the Active column.



The screenshot shows the 'User Management' page. At the top right is an 'Add User' button. Below it are tabs for 'Users', 'Correspondence Permissions', and 'Domain Management'. A search bar is present with a dropdown for 'Search By Name or Email' and a search icon. To the right of the search bar is an 'Export All to Worksheet' button. Below the search bar is a table with columns: LAST NAME, FIRST NAME, EMAIL, ORG ROLE(S), ACTIVE, and LAST LOGIN. The table contains four rows of user data. The first three rows show users with the role 'Admin' and a lock icon in the 'ACTIVE' column, indicating they are locked. The fourth row shows a user with the role 'Admin' and a checkmark in the 'ACTIVE' column, indicating they are active. The 'LAST LOGIN' column shows the last login time for each user.

LAST NAME	FIRST NAME	EMAIL	ORG ROLE(S)	ACTIVE	LAST LOGIN
4			Admin	🔒	Never
SA			Admin	🔒	04/27/24 01:34:39
JA			Admin	🔒	04/24/24 15:26:55
RC			Admin	✓	07/25/24 14:51:41

Figure 1.45: User Management.

2. Select the account that needs to be unlocked. Within the user's account, click the **kebab menu** at the right corner and select Unlock User Account.

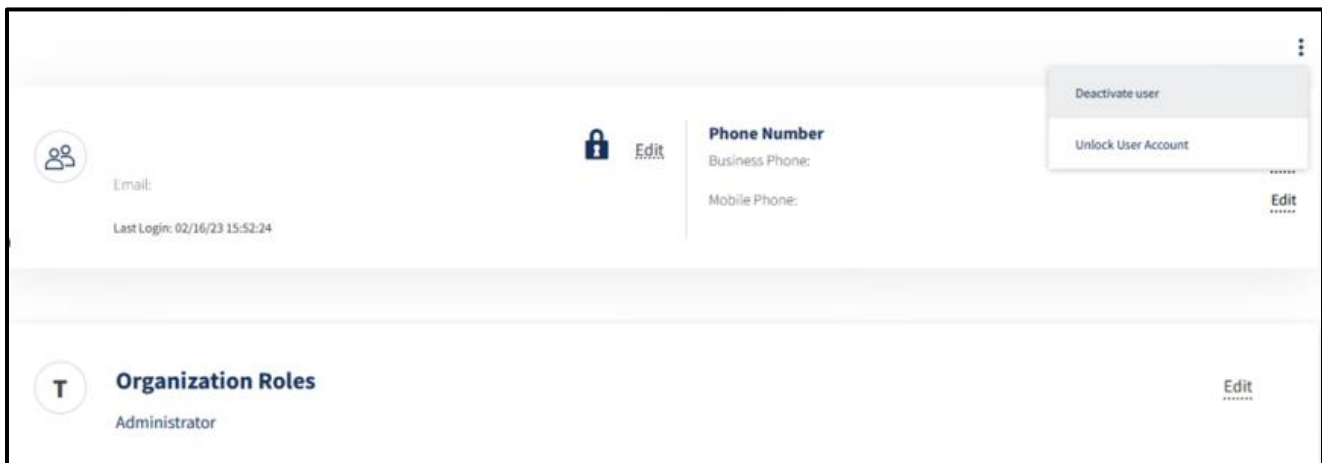


Figure 1.46: Unlock User Account.

Provider Portal User Guide: Provider Organization

Page updated: September 2024

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

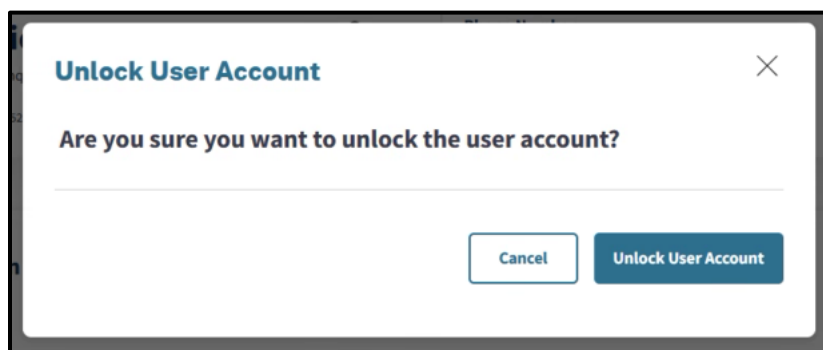


Figure 1.47: Unlock User Account.

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

Going Paperless

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

1. From the home page of the Portal, click **Edit** in the **My Profile and Preferences** area. A page to **Edit My Account Information** appears.

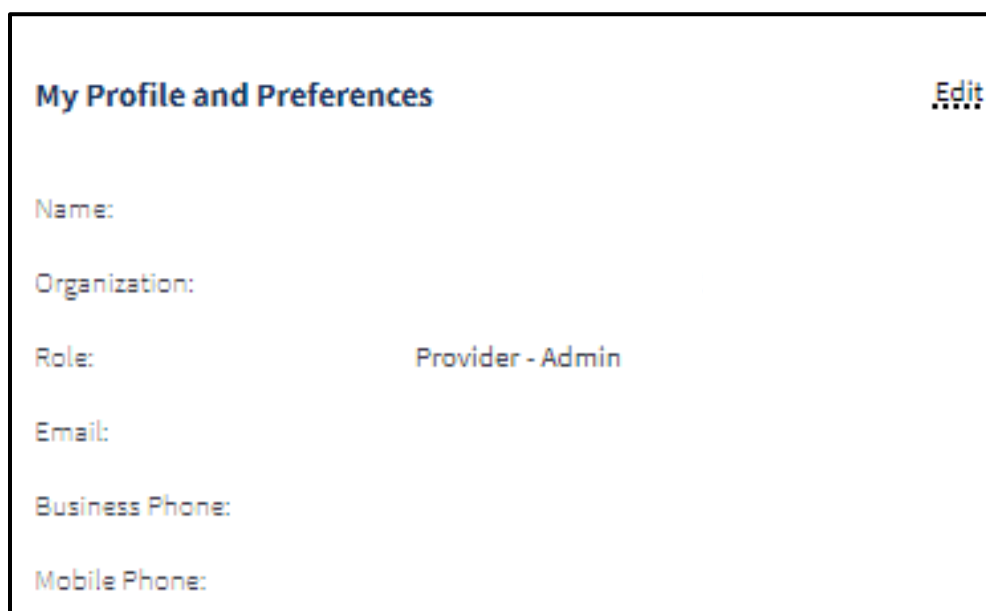
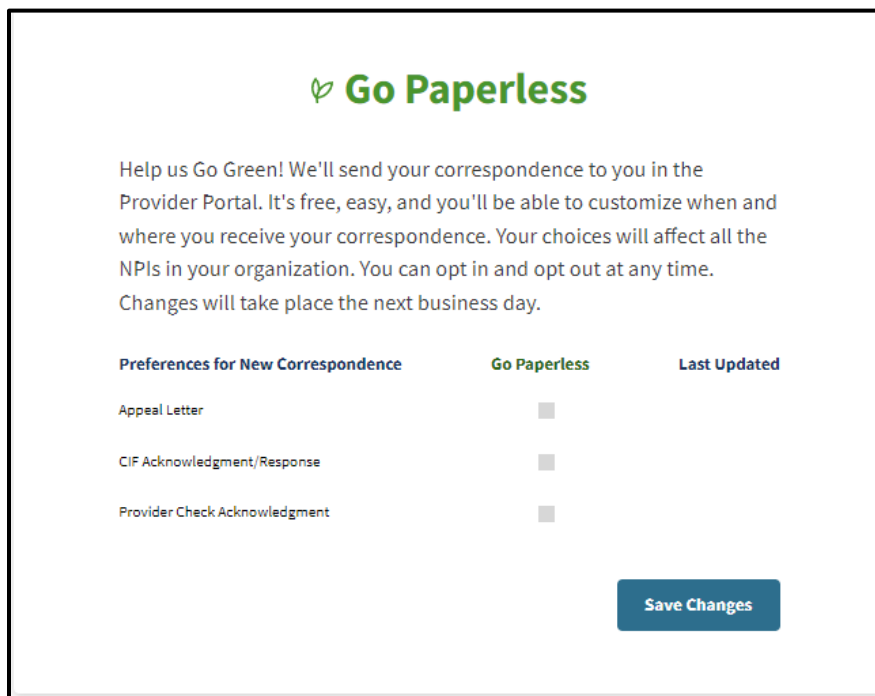


Figure 1.48: My Profile and Preferences.

Provider Portal User Guide: Provider Organization

Page updated: March 2024

2. Scroll down to **Go Paperless**.



Go Paperless

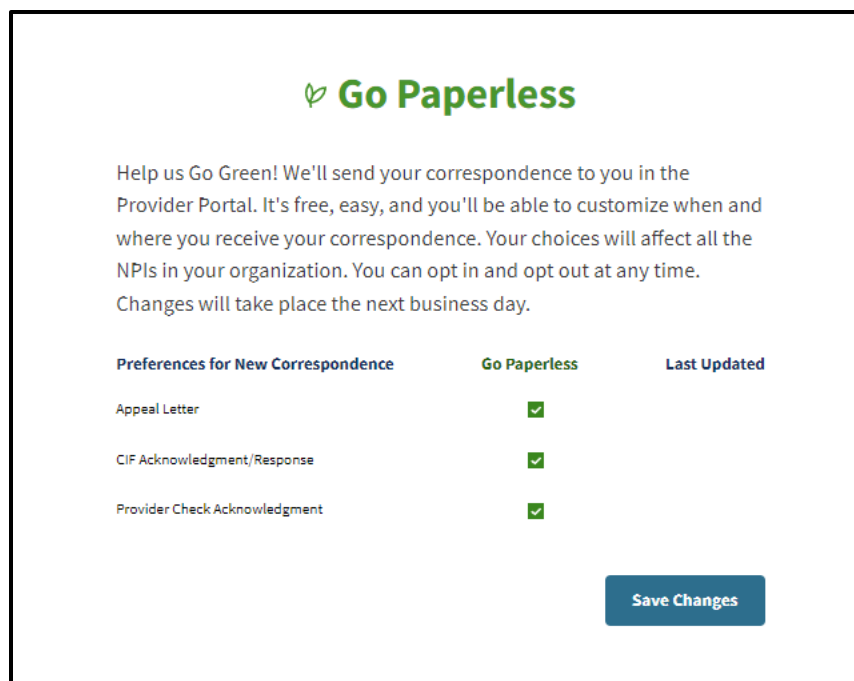
Help us Go Green! We'll send your correspondence to you in the Provider Portal. It's free, easy, and you'll be able to customize when and where you receive your correspondence. Your choices will affect all the NPIs in your organization. You can opt in and opt out at any time. Changes will take place the next business day.

Preferences for New Correspondence	Go Paperless	Last Updated
Appeal Letter	<input type="checkbox"/>	
CIF Acknowledgment/Response	<input type="checkbox"/>	
Provider Check Acknowledgment	<input type="checkbox"/>	

[Save Changes](#)

Figure 1.49: Go Paperless.

3. Check the Go Paperless box next to the preferred correspondence and click **Save Changes**.



Go Paperless

Help us Go Green! We'll send your correspondence to you in the Provider Portal. It's free, easy, and you'll be able to customize when and where you receive your correspondence. Your choices will affect all the NPIs in your organization. You can opt in and opt out at any time. Changes will take place the next business day.

Preferences for New Correspondence	Go Paperless	Last Updated
Appeal Letter	<input checked="" type="checkbox"/>	
CIF Acknowledgment/Response	<input checked="" type="checkbox"/>	
Provider Check Acknowledgment	<input checked="" type="checkbox"/>	

[Save Changes](#)

Figure 1.50: Go Paperless enrollment.

Provider Portal User Guide: Provider Organization

Page updated: March 2024

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

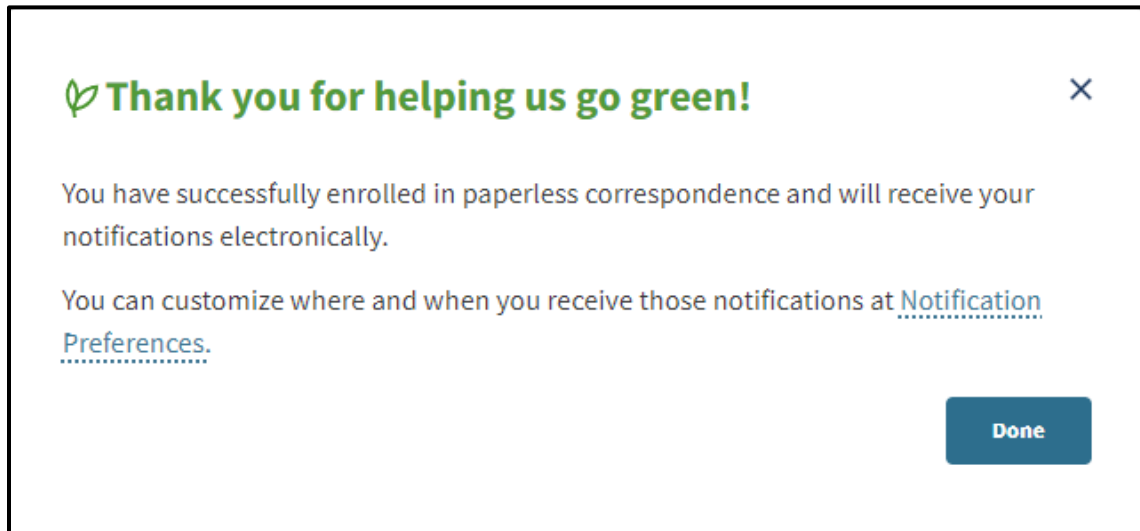


Figure 1.51: Go Paperless enrollment confirmation.

Provider Portal Features

The Provider Portal consolidates Medi-Cal-related information for the user's organization into a single **Dashboard**. See each section below for details on how to use each of the Provider Portal areas.

My Profile and Preferences

The **My Profile** tile houses personal account information and notification preferences. To edit a user's information and preferences, click **Edit** in the **My Profile and Preferences** tile on the **Dashboard**:

A screenshot of a web form titled "My Profile and Preferences" in blue text. In the top right corner, there is a blue "Edit" link. The form contains several labels: "Name:", "Organization:", "Role:", "Email:", "Business Phone:", and "Mobile Phone:". The "Role:" field is populated with the text "Provider - Admin".

Figure 2.1: My Profile and Preferences.

Edit Personal Information

Personal information can be updated at any time. Follow the steps below:

1. Click **Edit** next to **Personal Information**.

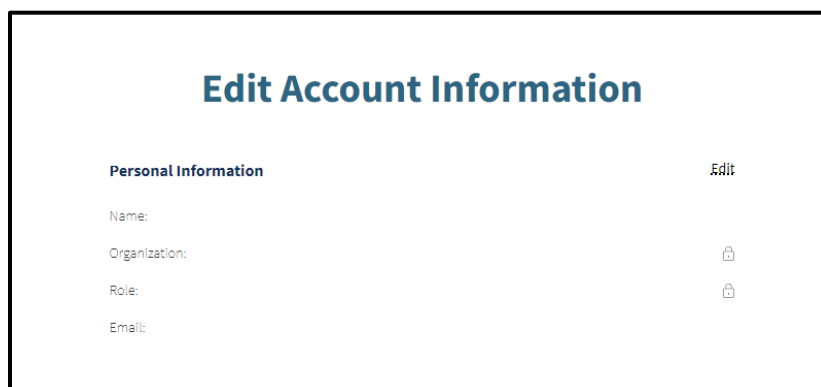
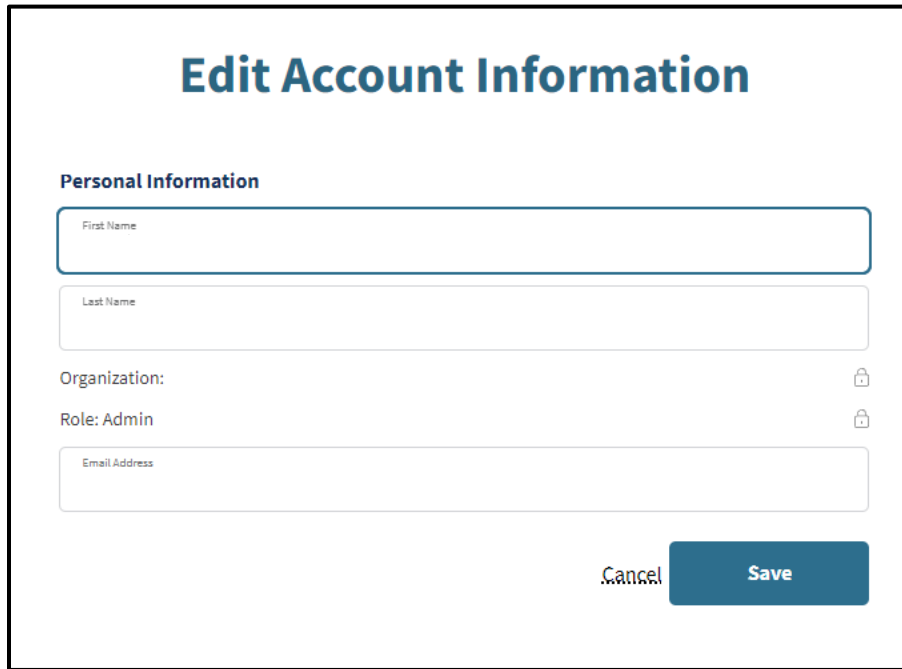
A screenshot of a web form titled "Edit Account Information" in blue text. Below the title is a section header "Personal Information" in blue. To the right of this header is a blue "Edit" link. The form contains labels for "Name:", "Organization:", "Role:", and "Email:". To the right of the "Organization:", "Role:", and "Email:" labels are small lock icons, indicating that these fields are locked for editing.

Figure 2.2: Edit Account Information.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

2. Update the desired information and click **Save**.



The screenshot shows a form titled "Edit Account Information" in a large blue font. Below the title is a section header "Personal Information" in a smaller blue font. The form contains several input fields: "First Name" and "Last Name" are text boxes; "Organization:" and "Role: Admin" are labels followed by fields with lock icons on the right, indicating they are read-only; "Email Address" is a text box. At the bottom right of the form are two buttons: "Cancel" and "Save".

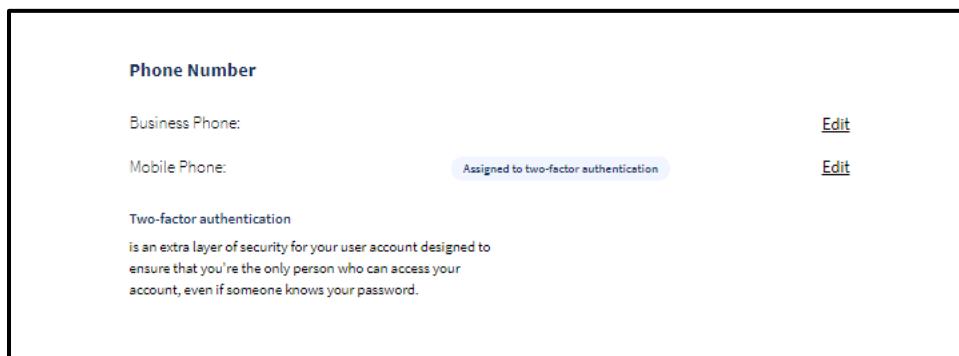
Figure 2.3: Edit Personal Information.

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. **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.

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

Edit Phone Number

1. Click **Edit** next to the phone number to edit.



The screenshot shows a section titled "Phone Number" in blue. It contains two rows of information: "Business Phone:" with an "Edit" link to its right, and "Mobile Phone:" with a blue pill-shaped label "Assigned to two-factor authentication" and an "Edit" link to its right. Below this is a section titled "Two-factor authentication" in blue, followed by a paragraph: "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 2.4: Phone Number.

Provider Portal User Guide: Provider Organization

Page updated: September 2024

2. From there, the field opens allowing the user to edit the phone number. If the phone number selected is not assigned to two-factor authentication and the user would like to use two-factor authentication, click **Use this number for two step authentication**.

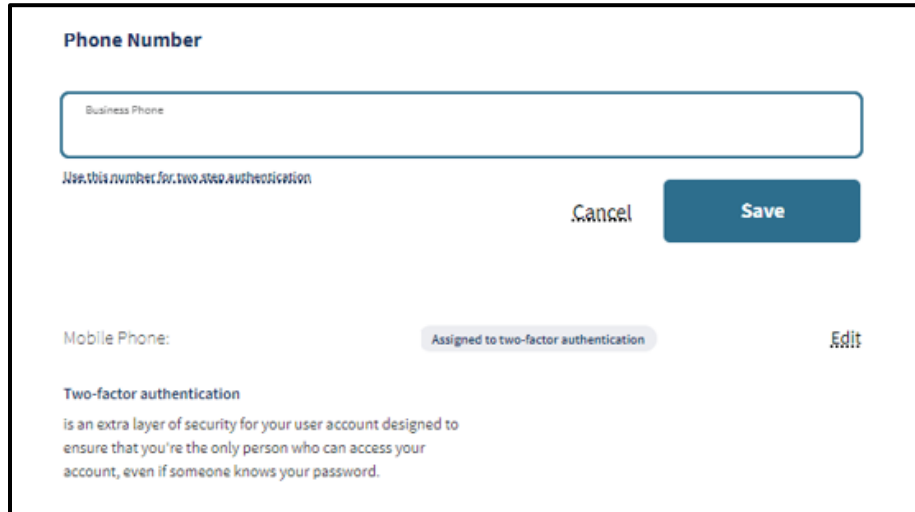
The screenshot shows a 'Phone Number' edit form. At the top, there's a title 'Phone Number'. Below it is a text input field labeled 'Business Phone'. Under the input field, there's a link that says 'Use this number for two step authentication'. To the right of the link are two buttons: 'Cancel' and 'Save'. Below the input field, there's a section for 'Mobile Phone:' which shows 'Assigned to two-factor authentication' and an 'Edit' link. At the bottom, there's a section for 'Two-factor authentication' with a descriptive paragraph: '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 2.5: Edit Phone Number.

3. Click **Save**. The phone number is now updated.

Edit Passkey

1. Click **Edit** in the User Passkey area.

The screenshot shows a 'User Passkey' edit form. At the top, there's a title 'User Passkey' with a help icon. To the right of the title is an 'Edit' link. Below the title, it says 'Passkey not set'.

Figure 2.6: Edit Passkey.

Provider Portal User Guide: Provider Organization

Page updated: September 2024

2. After entering the One-Time Passcode, enter a four (4) digit passkey. It is important to remember the passkey as it will be needed to reset passwords with help desk and for security verification.

A screenshot of a web form titled "User Passkey" with a help icon. The form contains two input fields, each with a placeholder "Insert" and a toggle icon. The first field is labeled "Enter 4 digit User Passkey" and the second is labeled "Retype 4 digit User Passkey". At the bottom right, there are two buttons: "Cancel" and "Save Changes".

Figure 2.7: Edit Passkey.

3. Once complete, the "Successfully updated user passkey" message will appear.

A screenshot of the "User Passkey" page. At the top left is the title "User Passkey" with a help icon. At the top right is an "Edit" link. Below the title, there are four asterisks "****" representing a masked passkey. A green banner at the bottom of the form area contains the text "Successfully updated user passkey".

Figure 2.8: Successfully Updated User Passkey.

Provider Portal User Guide: Provider Organization

Page updated: September 2024

Edit NPI Preferences

A default NPI will be automatically selected when completing tasks for transactions, correspondence and more. To edit the NPI Preferences, a user can select a different NPI from the drop-down menu and then click **Save Changes**.

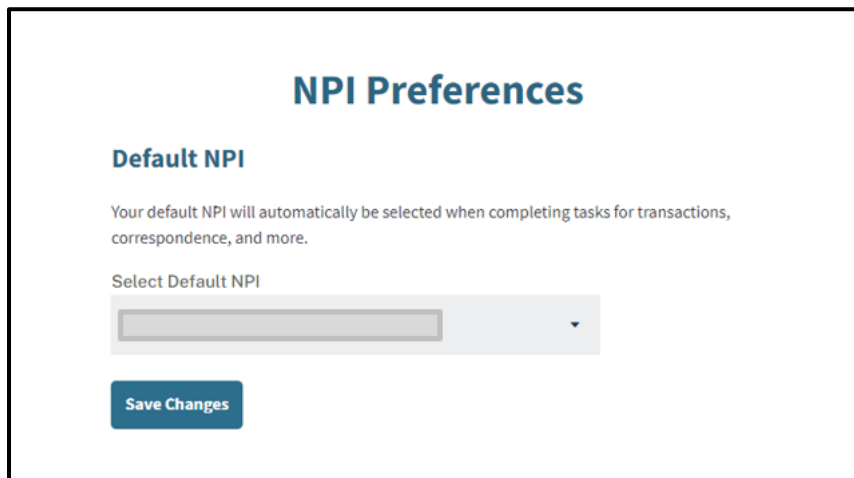


Figure 2.9: NPI Preferences.

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 receiving them on paper in the mail.

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

Enrolling

1. Click **Edit** under Electronic Tax Documents Enrollment.



Figure 2.10: Edit Electronic Tax Documents Enrollment.

2. The Electronic 1099 Consent: Unenrolled page opens. From here, click the **Go to Correspondence Center** button to navigate to the area where the user can give consent to receive electronic tax documents.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

The screenshot shows a white rectangular box with a black border. At the top, the title "Electronic 1099 Consent: Unenrolled" is displayed in a bold, dark blue font. Below the title, a paragraph of text states: "You have not provided your consent to receive electronic 1099s. You may enroll at any time in the tax documents section of the Correspondence Center." A horizontal line separates this text from the bottom section. In the bottom left, the text "Not Enrolled" is shown. In the bottom right, there is a blue rectangular button with the text "Go to Correspondence Center" in white.

Figure 2.11: Electronic 1099 Consent.

3. The Correspondence Center automatically opens to the Tax Documents area. Read the Electronic 1099 Consent Agreement, and then click the **I Have Read and Agree to The Above** button.

The screenshot shows a web interface for the "Tax Documents" section. At the top left, "Tax Documents" is written in a light blue font. Below this is a dark blue header bar. On the left side of the header bar, the text "Electronic 1099 Consent Agreement" is written in white. On the right side of the header bar, there is a radio button icon followed by the text "Not Signed". The main content area has a white background. It starts with the text "I acknowledge and agree to the following on behalf of my organization:". Below this is a numbered list of eight items, each followed by a period. The items describe the terms of the electronic 1099 consent, including the ability to withdraw consent, the availability of paper copies, and the requirements for accessing electronic 1099s. At the bottom of the main content area, there are two buttons. The first button is light blue with the text "I Do Not Agree" and a dotted underline. The second button is dark blue with the text "I Have Read and Agree to The Above" in white.

Figure 2.12: Electronic 1099 Consent Agreement.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

4. Once clicked, the user is successfully enrolled to receive electronic 1099s. While a confirmation screen does not appear, the user may check enrollment status by navigating back to the My Profile, clicking **Edit**, and scrolling to the Electronic Tax Documents Enrollment where it displays Electronic 1099s: *Enrolled*.

Withdrawing Enrollment

1. Click **Edit** under Electronic Tax Documents Enrollment.



Figure 2.13: Edit Electronic Tax Documents Enrollment.

2. The Electronic 1099 Consent page opens. Click the **Withdraw Consent and Receive Paper 1099s** button.

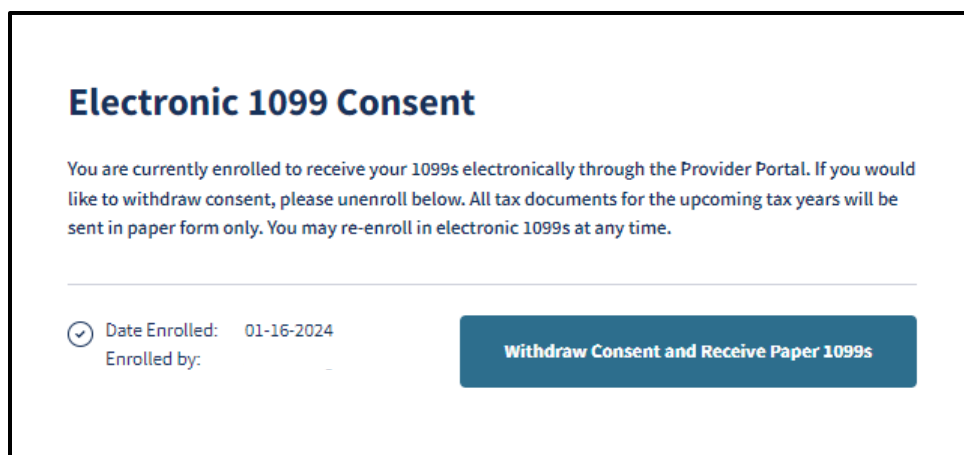
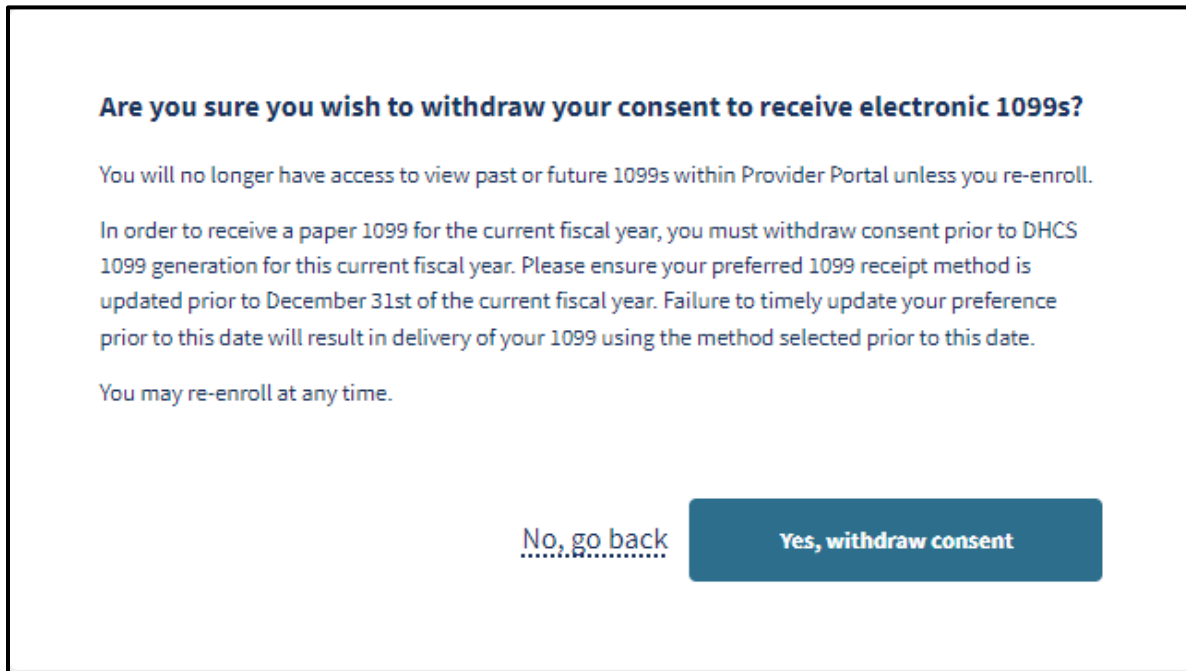


Figure 2.14: Electronic 1099 Consent Withdrawal.

Provider Portal User Guide: Provider Organization

Page updated: March 2024

3. A page appears verifying that the user would like to receive paper 1099s. Click the **Yes, withdraw consent** button to confirm disenrollment.



Are you sure you wish to withdraw your consent to receive electronic 1099s?

You will no longer have access to view past or future 1099s within Provider Portal unless you re-enroll.

In order to receive a paper 1099 for the current fiscal year, you must withdraw consent prior to DHCS 1099 generation for this current fiscal year. Please ensure your preferred 1099 receipt method is updated prior to December 31st of the current fiscal year. Failure to timely update your preference prior to this date will result in delivery of your 1099 using the method selected prior to this date.

You may re-enroll at any time.

[No, go back](#) **Yes, withdraw consent**

Figure 2.15: Withdraw consent to receive electronic 1099s.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

4. Once confirmed, the user is successfully disenrolled from receiving electronic 1099s. While a confirmation screen does not appear, the user may check enrollment status by navigating back to the My Profile, clicking **Edit**, and scrolling to the Electronic Tax Documents Enrollment where it displays Electronic 1099s: *Not Enrolled*.

Edit Notification Preferences

Users automatically receive notifications in the Provider Portal via the **Notifications** area. See the “Notifications” section of this user guide for the types of notifications the user may receive in the Provider Portal. This setting is automatically selected and cannot be changed. However, if a user would like to receive notifications via email, the user can select the **Email** checkbox next to the desired notification.

	Portal	Email	Email Frequency
New Correspondence			
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
User Activity			
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
Password			
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 2.16: Edit Notification Preferences.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

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

The screenshot shows a form titled 'New Correspondence' with three rows of notifications. Each row has checkboxes for 'Portal' and 'Email', and a dropdown menu for 'Email Frequency'. The 'Email Frequency' dropdown menu is open for the first row, showing options: Daily (selected), Weekly, Monthly, and Yearly.

	Portal	Email	Email Frequency
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"/>	✓ Daily
835 Receiver	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Weekly

Figure 2.17: Edit Notification Frequency.

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

The screenshot shows the same 'New Correspondence' form as Figure 2.17, but with a green confirmation message 'Preferences updated' at the top. The 'Email Frequency' dropdown menu is now closed and shows 'Daily'.

	Portal	Email	Email Frequency
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"/>	

Figure 2.18: Notification Preference successfully updated.

Transaction Center

Provider Portal users may access Transaction Services by secure single sign-on through the Transaction Center. Click the **Get Started** link within the Transaction Center tile on the Provider Portal **Dashboard**.

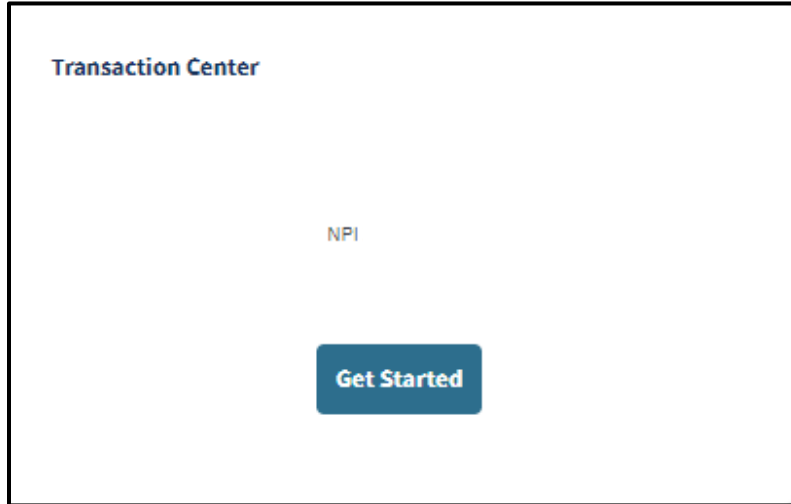


Figure 2.19: Transaction Center tile.

Provider Portal User Guide: Provider Organization

Page updated: March 2024

1. Once a user has entered the Transaction Center, a selection of links for various transactions will appear. Users may search or view transactions for the selected NPI.

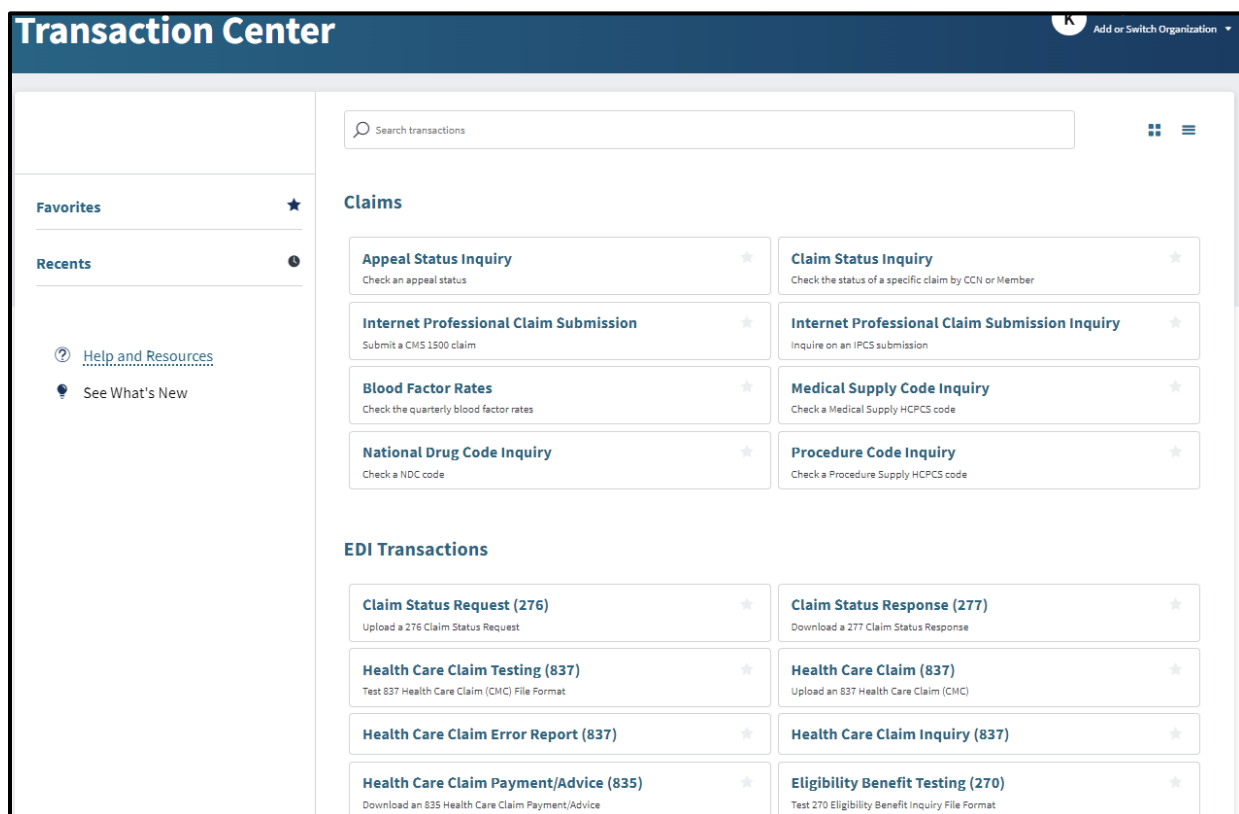


Figure 2.20: Transaction Center.

2. Users will be able to “Favorite” any transaction by clicking the star within each link, or previously selected transactions will be listed under the “Recents” heading.

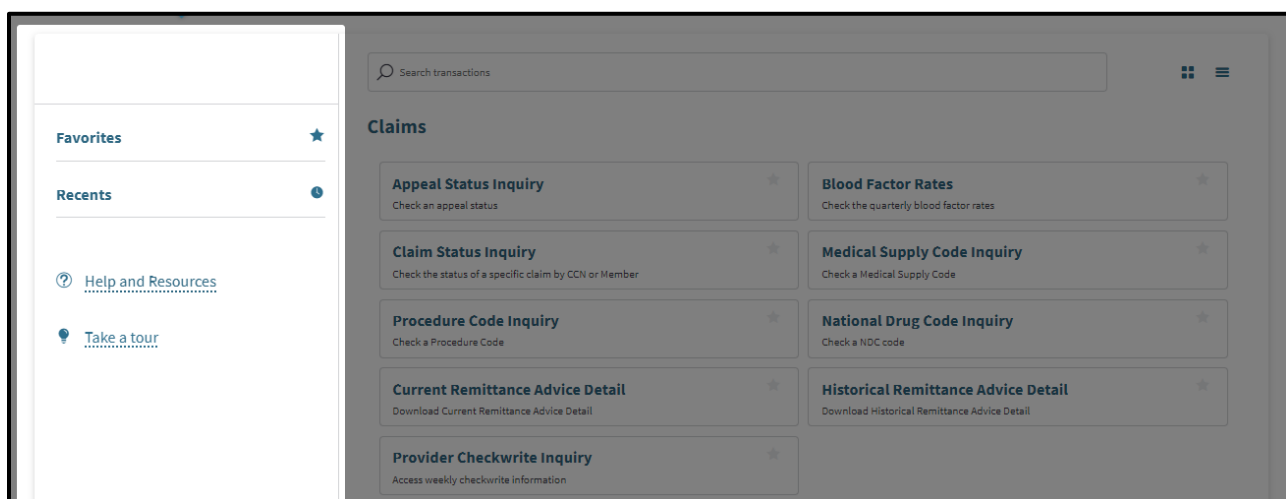


Figure 2.21: Side Panel Featuring Favorites and Recents.

Provider Portal User Guide: Provider Organization

Page updated: March 2024

Transaction Testing

1. To access Eligibility Benefit 270 Transaction Testing, click **Eligibility Benefit Testing (270)** under EDI Transactions. Once testing has been completed successfully, the link to submit production for EDI transactions will become available within the Transaction Center.

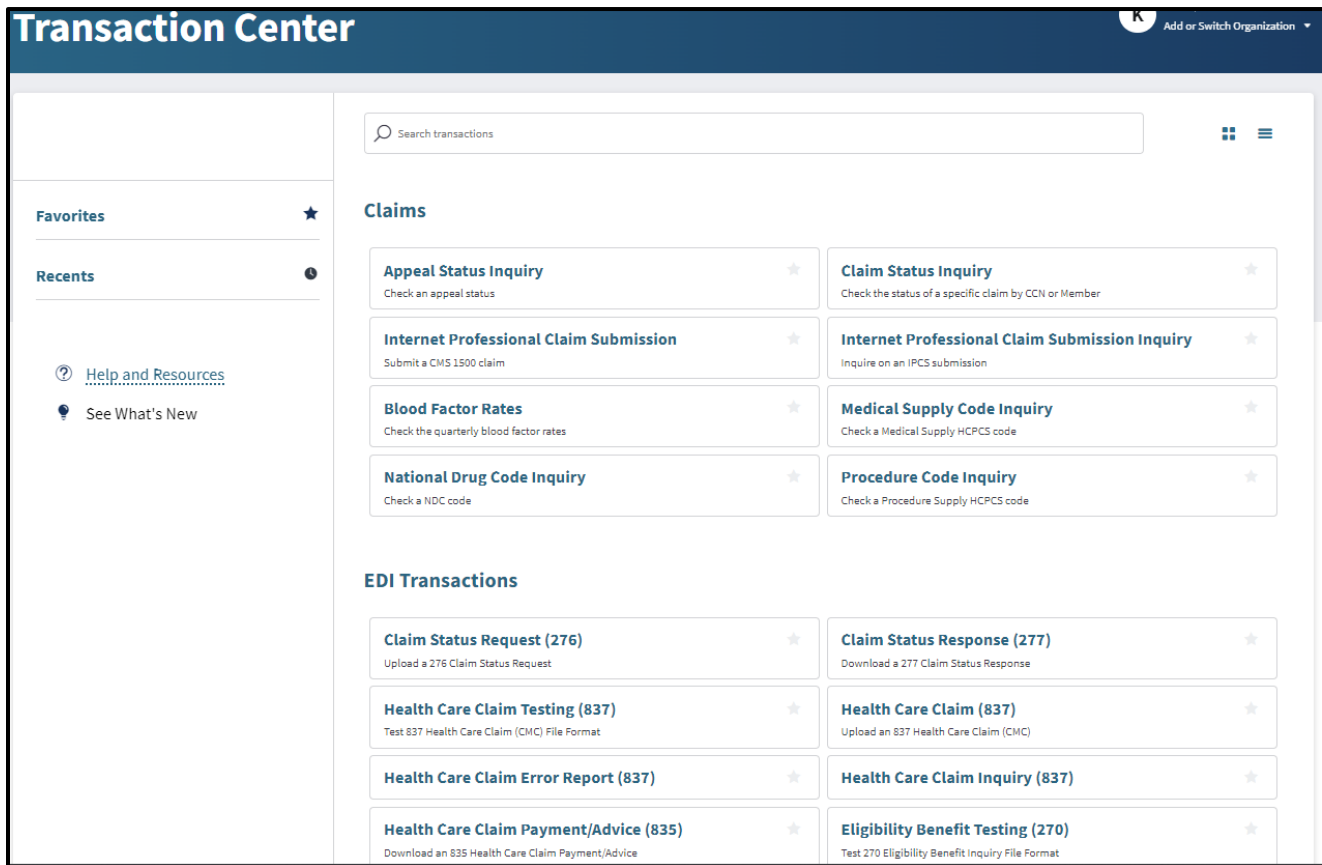


Figure 2.22: Transaction Center.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

2. Click **Upload a Submission** to upload a new test file.

The screenshot shows a web interface for 'Eligibility Benefit (270) Submissions'. On the left, a sidebar contains 'Submission Status' with details: 'Transaction Type: 270', 'Date: Still Pending', and 'Status: Not Started'. The main area has a title 'Eligibility Benefit (270) Submissions', a description 'View the status of 270 type test transactions. Test results may take up to 24 hours to be posted.', and instructions for new submitters. A blue 'Upload a Submission' button is on the right. At the bottom, a 'Need help?' section provides a link to instruction manuals.

Submission Status
Transaction Type:
270
Date:
Still Pending
Status: Not Started

Eligibility Benefit (270) Submissions
View the status of 270 type test transactions. Test results may take up to 24 hours to be posted.
New submitters must complete testing and activation procedures, located in the Medi-Cal Computer Media Claims (CMC) Billing and Technical Manual - Testing and Activation Procedures section.
[Upload a Submission](#)

Need help?
Please refer to our details instruction manuals for guidance on how to format your submission, testing and submission procedure, and more.
[Take me there](#) →

Figure 2.23: Eligibility Benefit (270) Submissions.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

3. Select **Drag and drop your files here or click to browse** to upload a file for approval. If approved, users will be able to submit the claim type for valid providers and the test results will be received within 24 hours.

Submission Status


Transaction Type:
270

Date:
Still Pending

Status: Not Started

Eligibility Benefit Submissions > **Batch Upload (270)**

Upload one file at a time for processing. Users are encouraged to ZIP files prior to processing. File uploads are limited to 5MB, as larger files will not be accepted. You will receive your test results within 24 hours.



Drag and drop your files here
or click to **browse**

Text file or ZIP
Max File Size: 5MB

Reminder: Each uploaded file will be issued a Volser number. Volser numbers may be used to check the status of your submission. Volser details may not be available for up to 24 hours after the submission is uploaded, and details are available for approximately 30 days.

Need help?
Please refer to our details instruction manuals for guidance on how to format your submission, testing and submission procedure, and more.


Take me there 

Figure 2.24: Eligibility Benefit (270) upload.

50

Provider Portal User Guide: Provider Organization

Page updated: July 2023

4. Complete will appear on the screen once the file has been uploaded.

The screenshot displays the 'Eligibility Benefit Submissions > Batch Upload (270)' interface. At the top, a text block explains the upload process: 'Upload one file at a time for processing. Users are encouraged to ZIP files prior to processing. File uploads are limited to 5MB, as larger files will not be accepted. You will receive your test results within 24 hours.' Below this, a file named 'ProviderB270Pass.txt' is shown in a light blue box with a document icon and a close 'X' button. A dark blue 'Submit File' button is positioned to the right. A dark blue banner at the bottom indicates the upload is 'Complete' for 'ProviderB270Pass.txt', accompanied by a progress bar and a checkmark icon. A final reminder states: 'Reminder: Each uploaded file will be issued a Volser number. Volser numbers may be used to check the status of your submission. Volser details may not be available for up to 24 hours after the submission is uploaded, and details are available for approximately 30 days.'

Figure 2.25: Eligibility Benefit (270) Submit File.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

5. Once the file is successfully uploaded, the Volume Serial (Volser) Number, File Name, File Size and Date Submitted will appear.

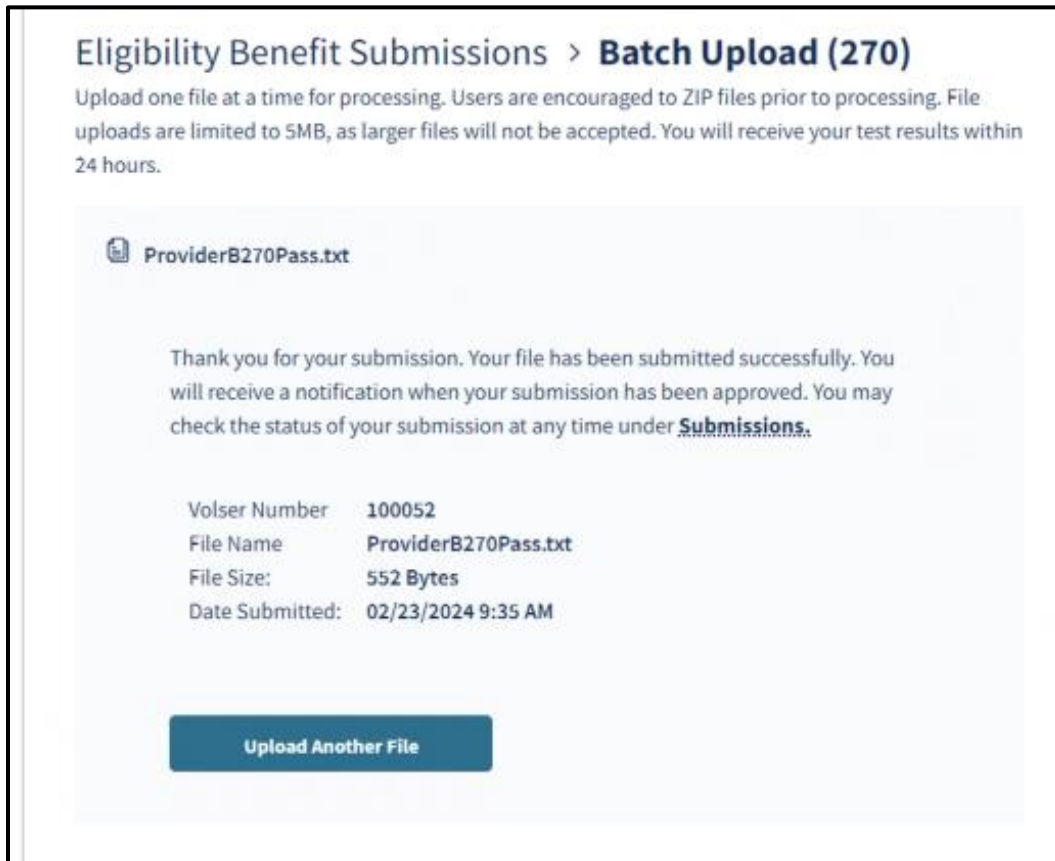


Figure 2.26: Eligibility Benefit (270) upload submission.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

6. Each file uploaded will be issued a Volser number.

Submission Status

Transaction Type:
270

Date:
Still Pending

Status: Pending

Eligibility Benefit (270) Submissions

View the status of 270 type test transactions. Test results may take up to 24 hours to be posted.

Reminder: Each uploaded file will be issued a Volser number. Volser numbers may be used to check the status of your submission. Volser details may not be available for up to 24 hours after the submission is uploaded, and details are available for approximately 30 days.

File Name	Volser No.	TA1 ACK	999 ACK	271 Response	Upload Date	Status
ProviderB270 Pass.txt	100050	Download	N/A	Download	02/22/2024 12:23 PM	Failed
ProviderB270 999ACK-Fail.txt	100051	Download	Download	N/A	02/22/2024 12:24 PM	Failed

Need help?
Please refer to our details instruction manuals for guidance on how to format your submission, testing and submission procedure, and more.
[Take me there](#)

Upload a New Submission

Figure 2.27: Eligibility Benefit (270) submissions list.

7. Users will have the option to download the **TA1 ACK**, **999 ACK** or **271 Response** to view the status details. Refer to the [Batch Eligibility Benefit Inquiry/Response Testing User Guide](#) to find out more information about the testing acknowledgments.

Administration

The **Administration** area allows for management of users in an organization. Tasks include adding/removing users, updating user permissions and viewing information about users in the organization.

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

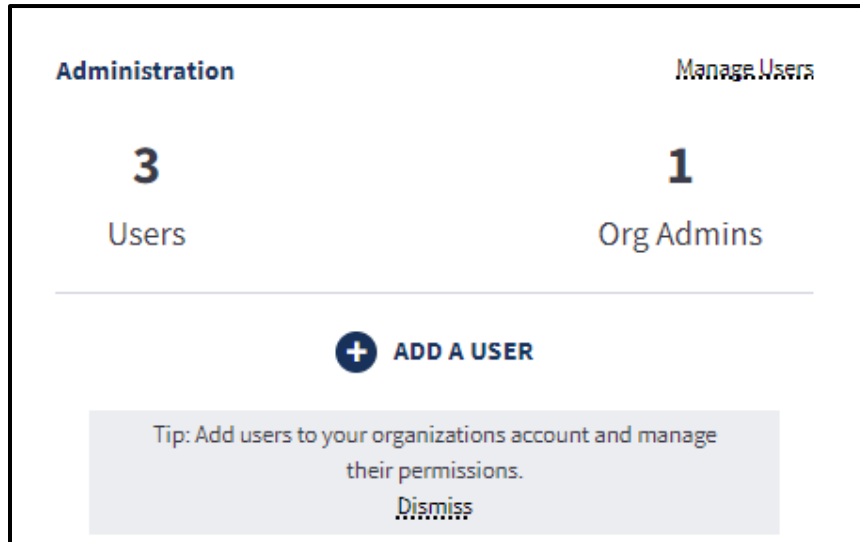


Figure 2.28: Administration Tile.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

Updating User Information/Permissions

To update user permissions after the initial assigning of permissions, follow these steps:

1. Click **Manage Users** on the dashboard.

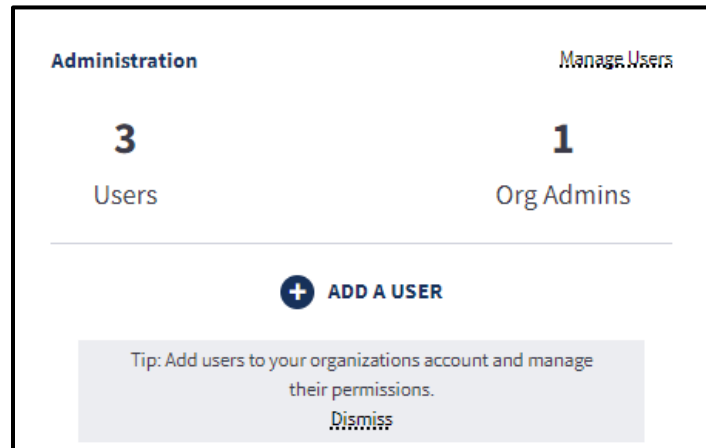


Figure 2.29: Administration Tile.

2. The user management area appears. Search for the user in the search box and click the row when it appears.

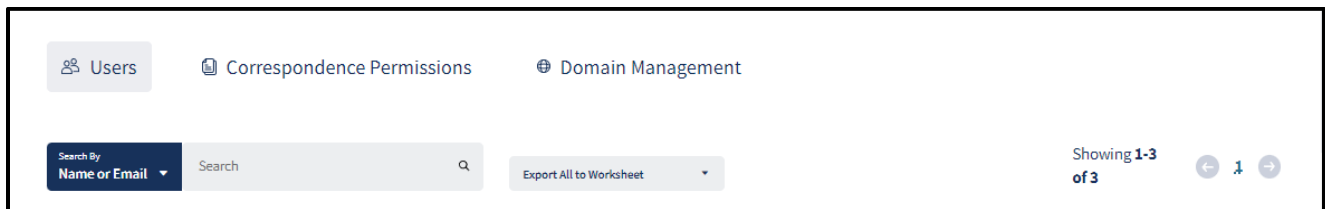


Figure 2.30: User Management.

3. The User Management and Permissions page appears. The NPI Permissions, Correspondence Permissions and Permissions Across Organization can be viewed and edited. Select **Edit** next to the permissions desired. For further steps, refer to the "Add User" section of this user guide.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

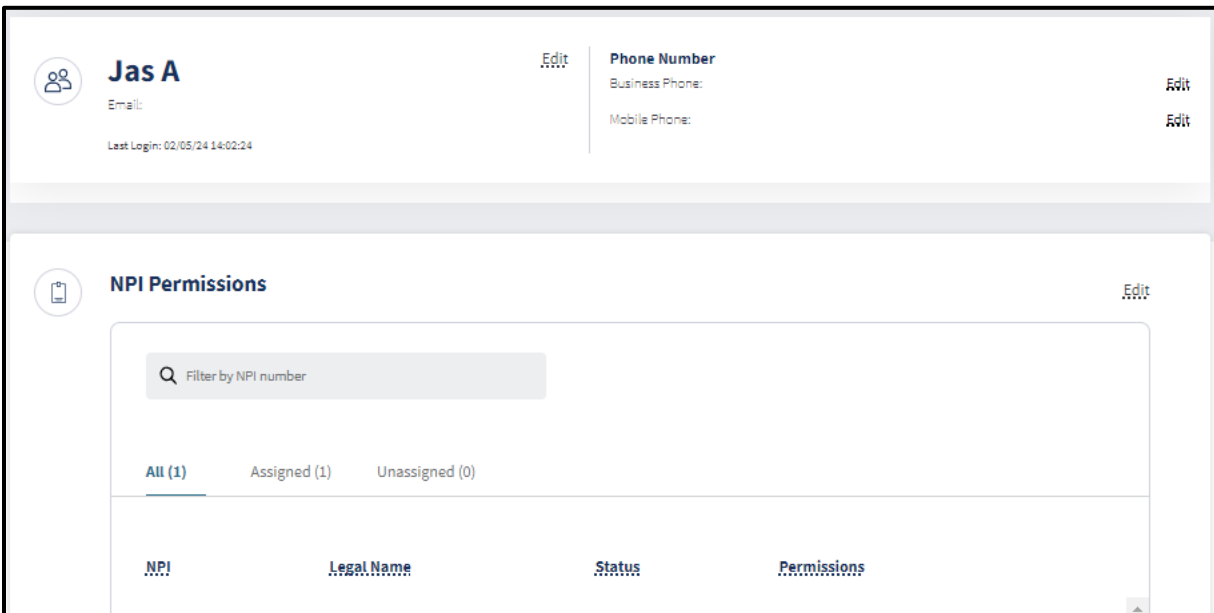


Figure 2.31: User Management and Permissions.

Deactivate User

Complete the following to deactivate a user:

1. On the **Dashboard**, select **Manage Users** contained in the **Administration** tile to open the user management area.

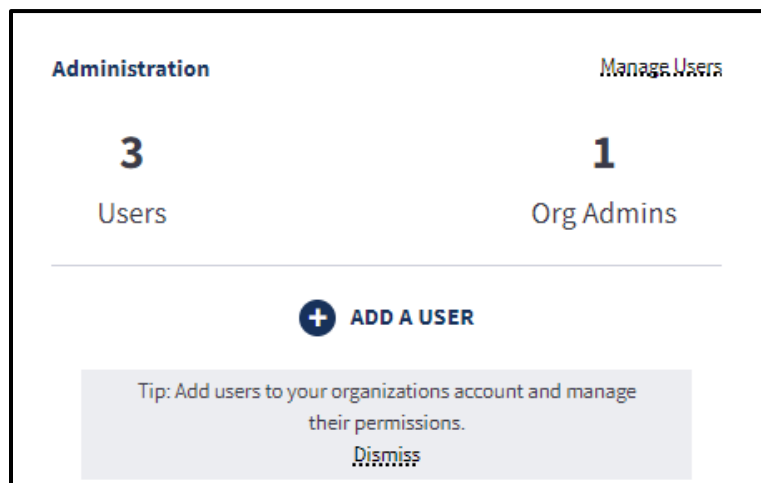


Figure 2.32: Administration Tile.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

2. In the search bar, search for the desired user to deactivate. Select the row that appears to open the user's information profile.

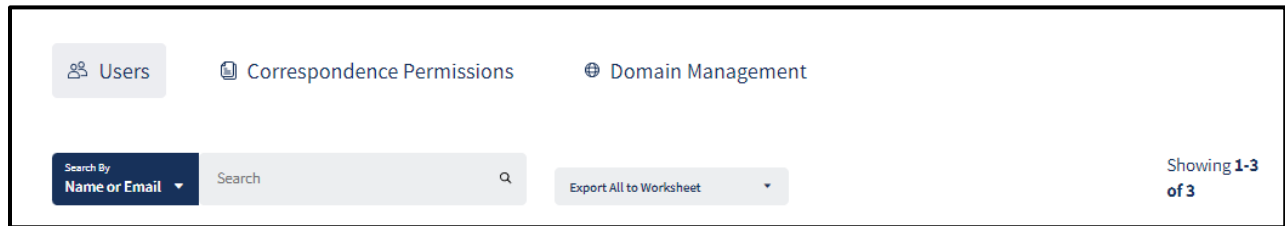


Figure 2.33: User Management.

3. At the top right corner of the user profile, select the **kebab menu** (three dots) in the top right corner. A link to **Deactivate User** appears.

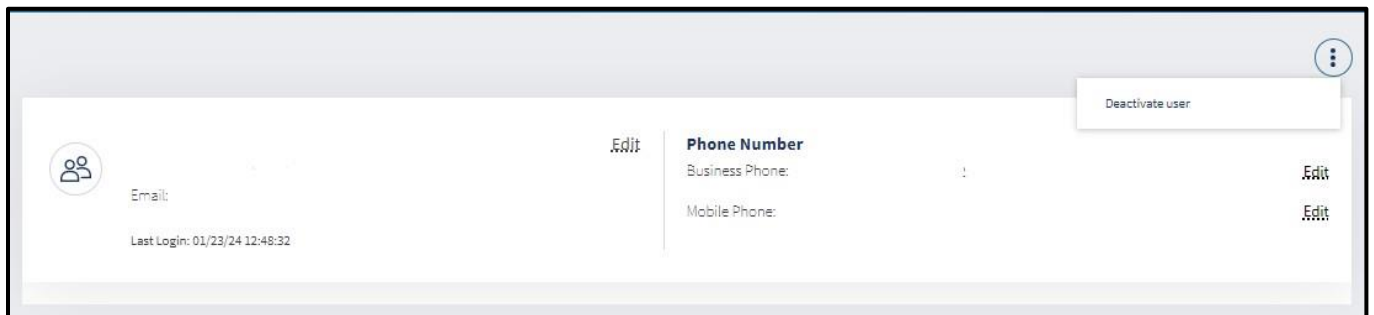


Figure 2.34: Deactivate User.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

4. Click **Deactivate User**. A pop-up window appears prompting to deactivate this user. Click **Confirm**.

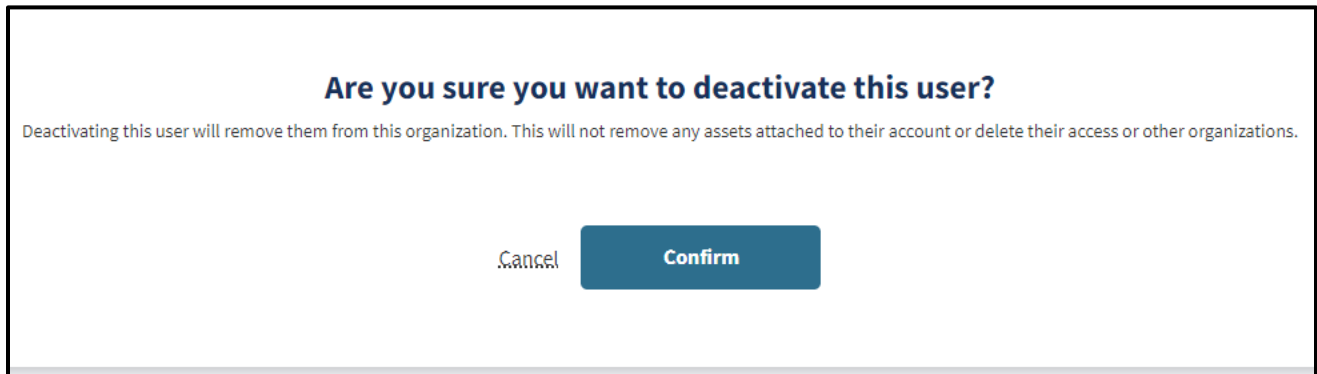


Figure 2.35: Confirmation to Deactivate User.

5. Once the confirm button has been selected, the user's profile displays, now with **Deactivated User** above the name. Users can be reactivated at any time.

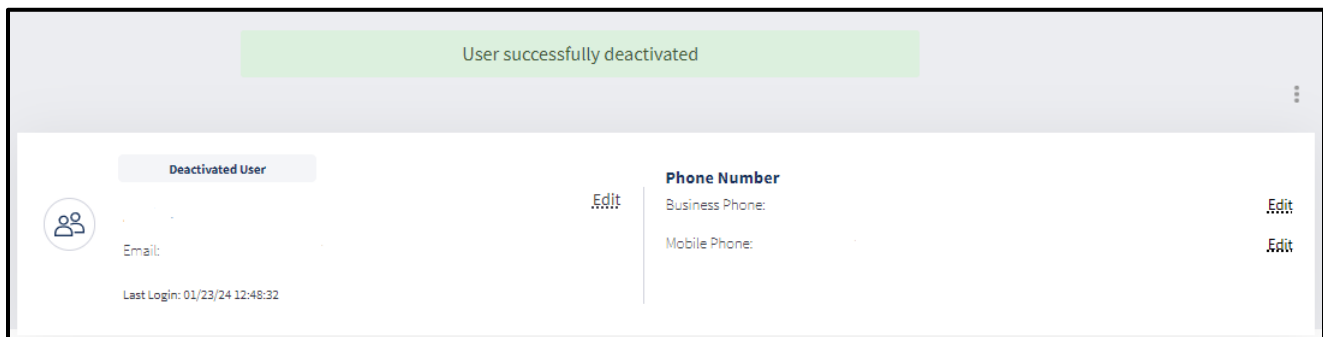


Figure 2.36: Deactivated User Messaging.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

Reactivate User

Complete the following to reactivate a user:

1. On the **Dashboard**, select **Manage Users** contained in the **Administration** tile to open the user management area.

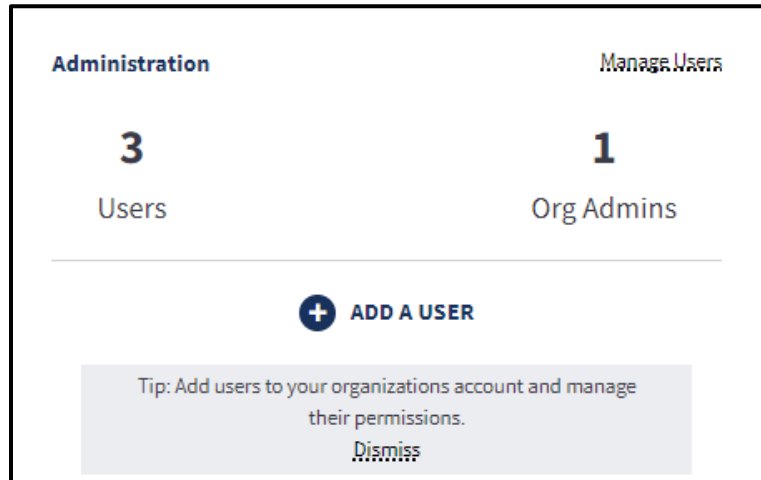


Figure 2.37: Administration Tile.

2. In the search bar, search for the desired user to reactivate. Select the row that appears to open the user's information profile.

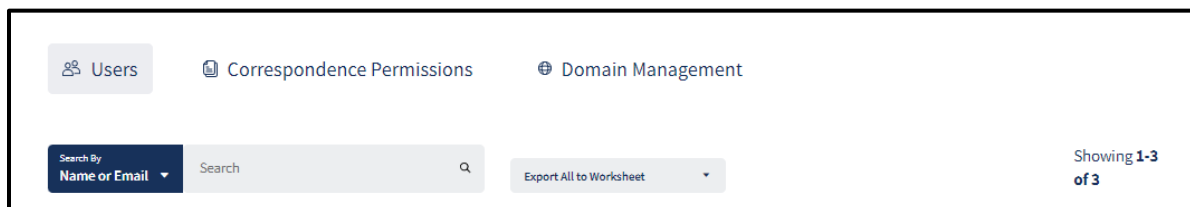


Figure 2.38: User Management.

3. At the top right corner of the user profile, select the **kebab menu** in the top right corner. A link to **Reactivate User** appears.

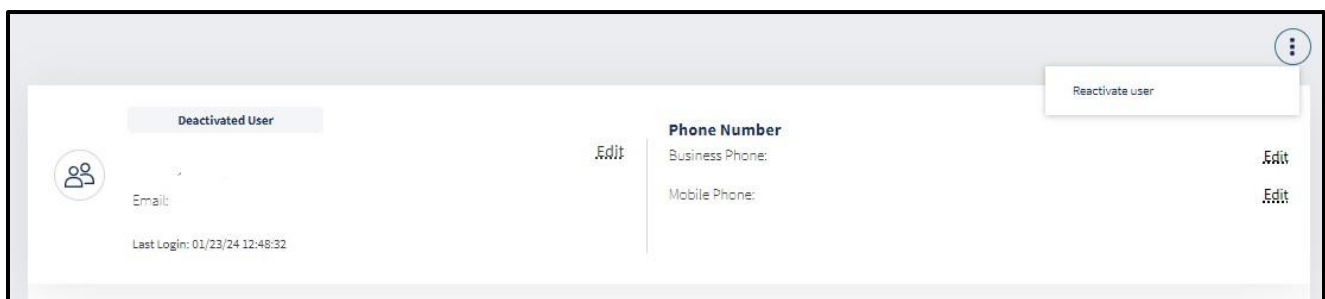


Figure 2.39: Reactivate User.

Provider Portal User Guide: Provider Organization

Page updated: March 2024

4. Click **Reactivate User**. A pop-up window appears prompting to reactivate this user. Click **Confirm**.

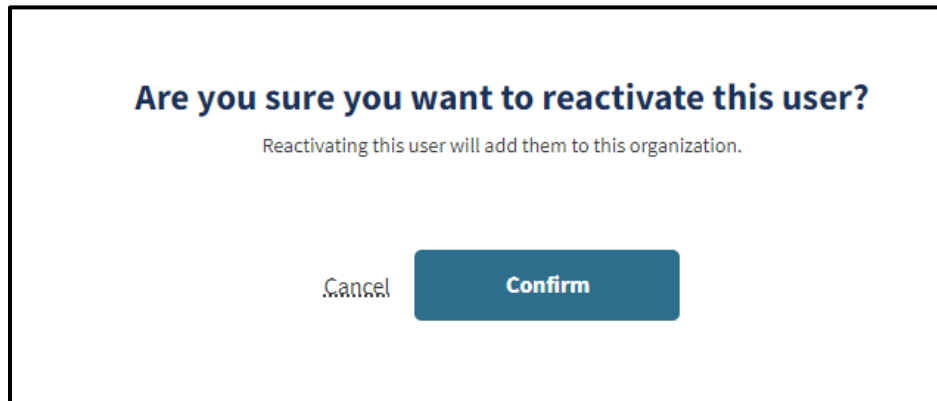


Figure 2.40: Reactivate User Confirmation.

5. Once the confirm button has been selected, the user's profile displays, now with **Reactivated User** above the name and the user is active again.

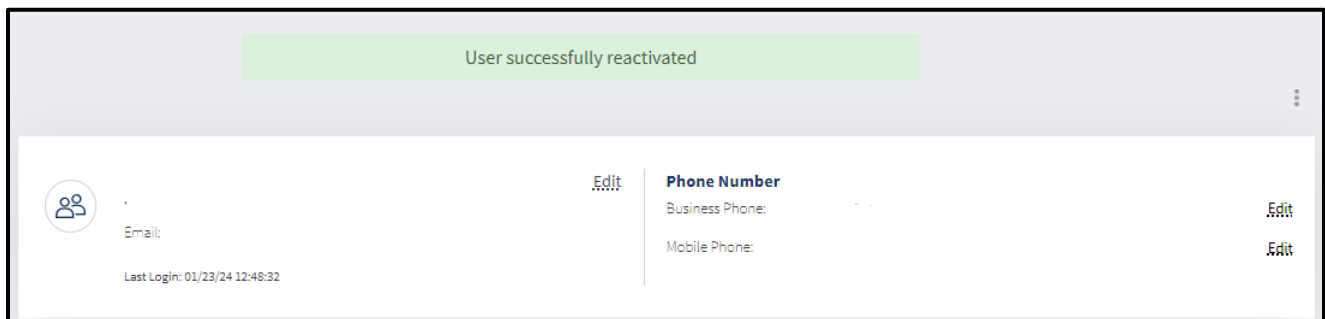


Figure 2.41: Reactivated User Messaging.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

Domain Management

To remove an unwanted domain from an organization, first ensure that there are no active users with that email address. If there are, those users must be deactivated first in order to remove the domain.

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

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

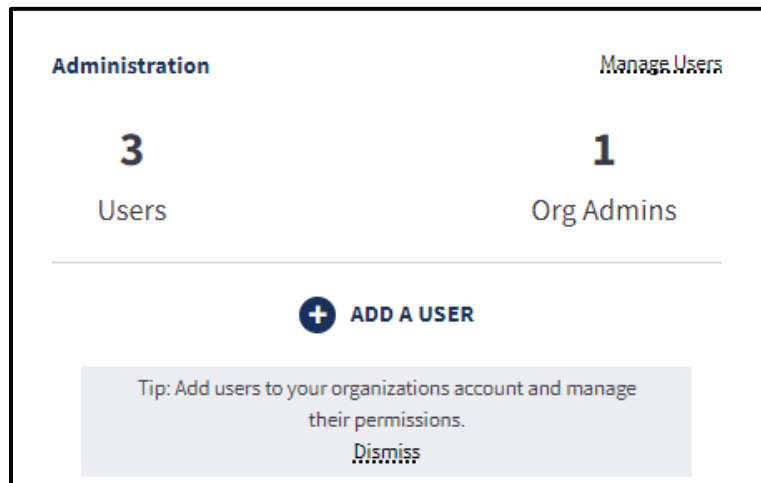


Figure 2.42: Administration Tile.

2. Click **Domain Management**.

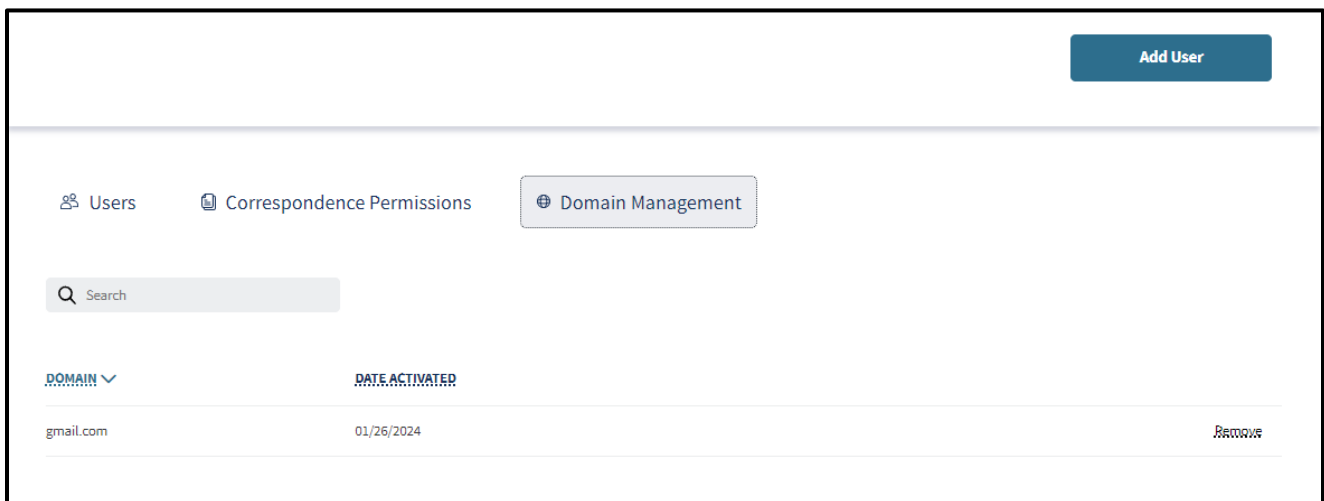


Figure 2.43: Domain Management.

3. Click **Remove** next to the domain that should be removed.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

Notifications

The **Notifications** area allows a user to quickly view notifications related to the organization. The most recent notifications appear on the dashboard. To see all notifications, click **View All**.

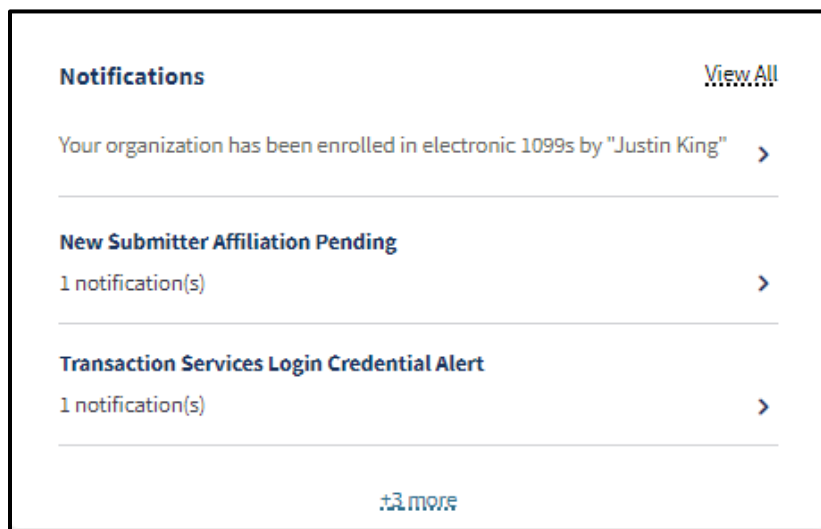


Figure 2.44: Notifications Tile.

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. To use the filter by date option, select the **Filter By Date** menu and enter the desired date range.

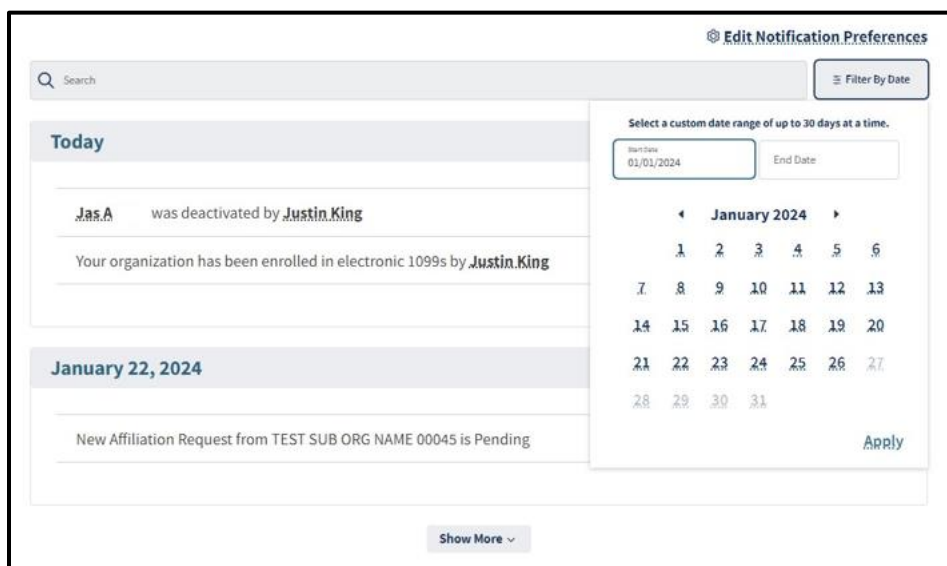


Figure 2.45: Filter by date for Notifications.

To edit notification preferences, click **Edit Notification Preferences**. Refer to the [Edit Notification Preferences](#) section in this user guide for detailed instructions.

Submitter Management

The Submitter Management area allows individuals designated as Organizational Administrators to submit or approve new affiliations with registered submitter organizations, view existing affiliation requests, manage submitter permissions and view the Submitter Directory.

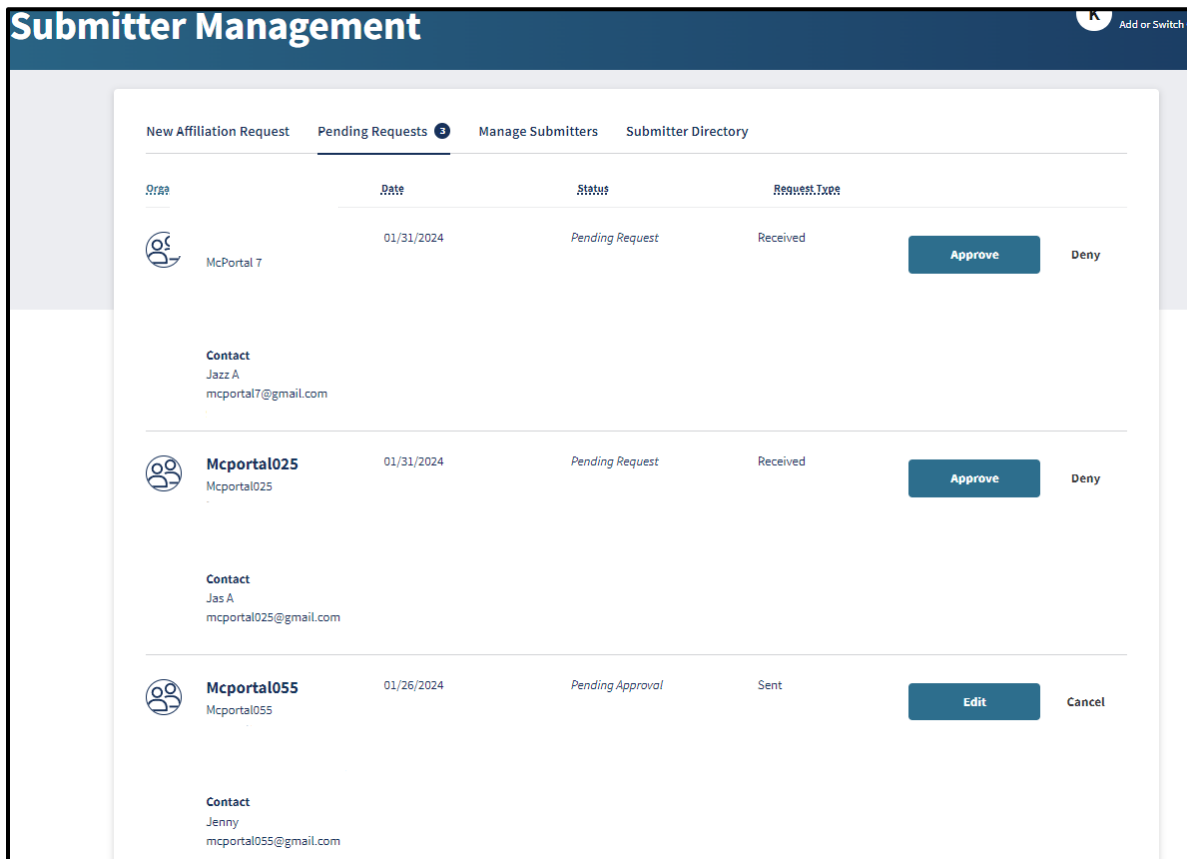


Figure 2.46: Pending Requests.

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

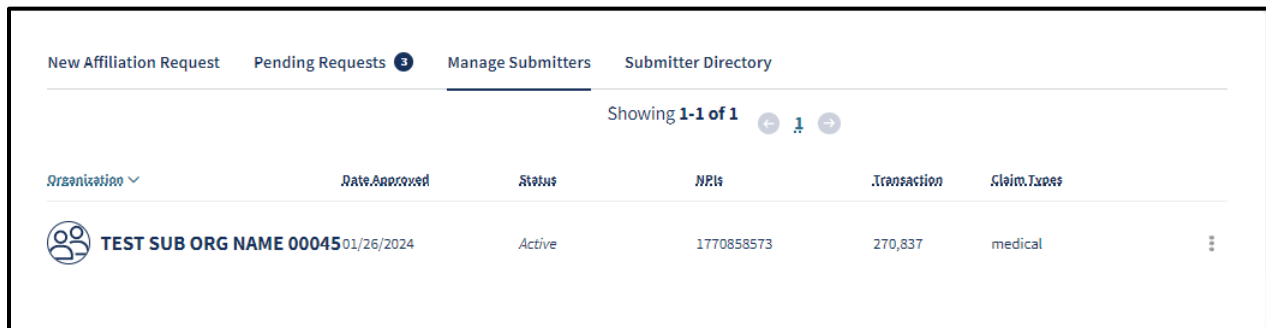


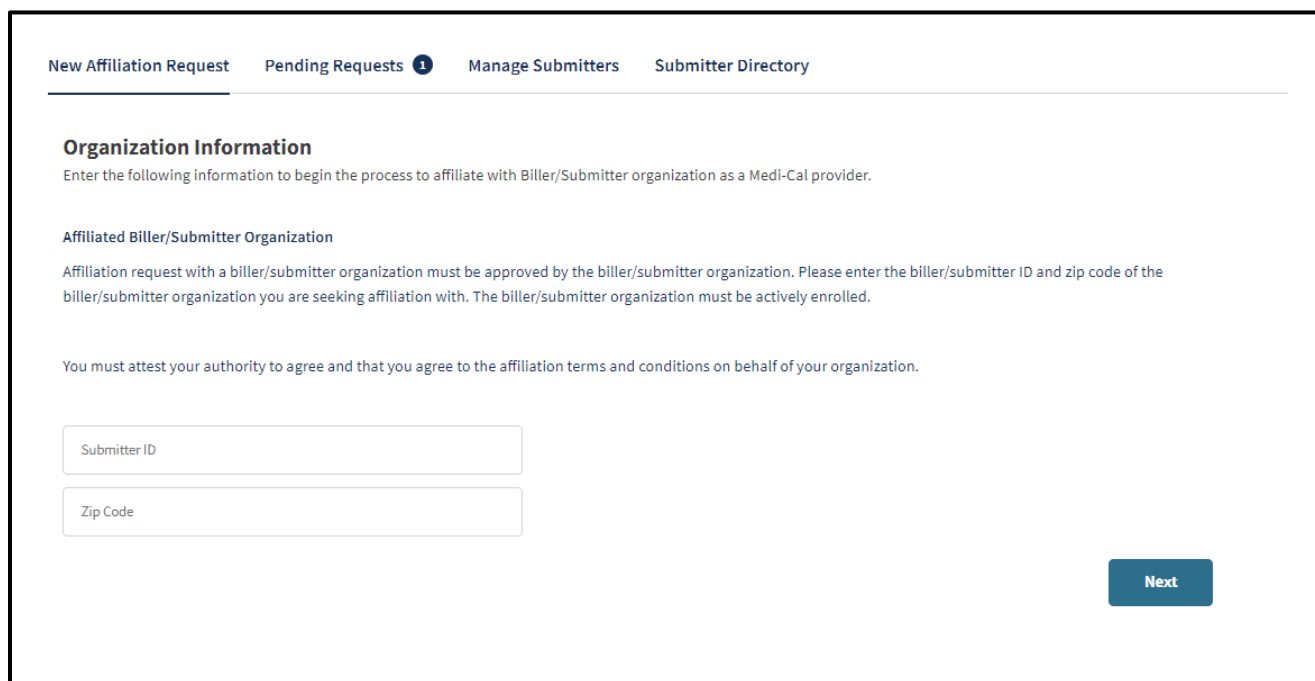
Figure 2.47: Manage Submitters.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

New Affiliation Request to a Submitter Organization

1. Under the **New Affiliation Request** tab, enter the **Organization Information (Submitter ID and Zip Code)** of the submitter organization. Click **Next** to continue.



The screenshot shows the 'New Affiliation Request' form. At the top, there are four tabs: 'New Affiliation Request' (selected), 'Pending Requests' (with a notification icon), 'Manage Submitters', and 'Submitter Directory'. Below the tabs, the section is titled 'Organization Information' with a sub-header 'Affiliated Biller/Submitter Organization'. The text explains that the affiliation request must be approved by the biller/submitter organization and that the biller/submitter organization must be actively enrolled. It also states that the user must attest their authority to agree to the affiliation terms and conditions on behalf of their organization. There are two input fields: 'Submitter ID' and 'Zip Code'. A blue 'Next' button is located at the bottom right of the form.

Figure 2.48: 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 an approval isn't received, the affiliation request can be resubmitted.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

2. Complete the *Medi-Cal Telecommunications Provider and Biller Application/Agreement* (DHCS 6153). Please read the agreement form and then sign with First and Last name along with Title. Once complete, click **Next**.

The screenshot shows the 'Medi-Cal Telecommunications Provider and Biller Application/Agreement' form. At the top, it states: 'DHCS and the California MMIS Fiscal Intermediary require a signed telecommunication application/agreement form from CMC submitters.' Below this is a header bar with 'Submitter + Provider Affiliation Agreement' on the left and two radio buttons on the right: 'TEST SUB ORG NAME 00045' (selected) and 'Not signed'. The main body of the form contains several sections of text, including '3.0 CLAIMS ACCEPTANCE AND PROCESSING', '3.1 CLAIMS CERTIFICATION', '3.2 VERIFICATION OF CLAIMS WITH SOURCE DOCUMENTS', and '3.3 ACCURACY AND CORRECTION OF CLAIMS OR PAYMENTS'. At the bottom, there is a checkbox labeled 'I confirm that I am eligible to sign this agreement on behalf of my organization'. Below the checkbox are two input fields: 'First and Last Name' and 'Title'. At the very bottom, it says 'I, the undersigned, am authorized and do attest and agree to all of the terms and conditions of this agreement.' followed by a line for 'Electronic Signature:'.

Figure 2.49: Medi-Cal Telecommunications Provider and Biller Application/Agreement.

3. A request complete screen will appear.

The screenshot shows a 'Request Complete' screen. At the top, the title 'Request Complete' is displayed in bold. Below the title, the text reads: '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.' At the bottom, there is a link labeled 'Back to Pending Requests'.

Figure 2.50: Request Complete.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

4. Once the submitter organization has signed the *Provider and Biller Application/Agreement*, the Administrator will receive an email confirmation for the approved affiliation request.

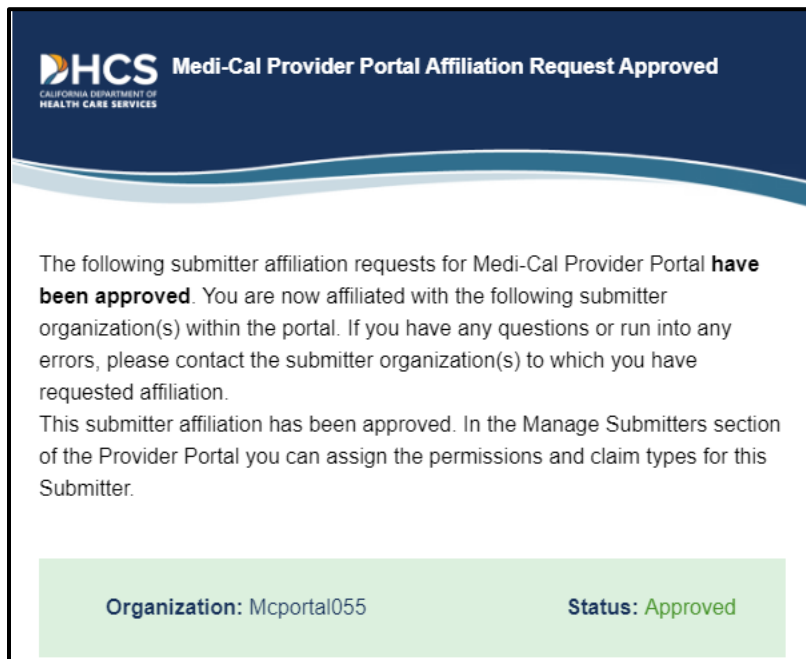


Figure 2.51: Email Confirmation for Approved Affiliation Request.

5. 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 [Manage Submitters](#) section for instructions about how to assign these permissions.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

Approve a Submitter Affiliation Request

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

The screenshot displays the 'Submitter Management' interface. At the top, there's a dark blue header with the title 'Submitter Management' and a user profile icon with the text 'Add or Switch User'. Below the header, there are four tabs: 'New Affiliation Request', 'Pending Requests' (which is active and has a blue circle with the number 3), 'Manage Submitters', and 'Submitter Directory'. The main content area shows a table of pending requests. Each row represents a request from a specific organization, with columns for Organization, Date, Status, and Request Type. For each request, there are 'Approve' and 'Deny' buttons. Below each request entry, there is a 'Contact' link.

Organization	Date	Status	Request Type
McPortal 7 McPortal 7	01/31/2024	Pending Request	Received
Approve Deny			
Contact			
Mcportal025 Mcportal025	01/31/2024	Pending Request	Received
Approve Deny			
Contact			
Mcportal055 Mcportal055	01/26/2024	Pending Approval	Sent
Edit Cancel			
Contact			

Figure 2.52: Pending Requests.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

2. Complete **Step 1: Assign NPI Permissions** by assigning the submitter to an NPI within the organization and click **Next**.

The screenshot shows the 'Step 1: Assign NPI Permissions' interface. At the top, the organization name 'TEST SUB ORG NAME 00045' is displayed next to a user icon. The user's name 'KING, JUSTIN B MD I...' is shown in the top right corner. Below the organization name, there are sections for 'Organization Information:' and 'Contact:'. The main heading 'Step 1' is followed by 'Assign NPI Permissions'. A sub-instruction reads: 'Assign this submitter to NPIs within this organization. All NPIs do not have to be assigned.' Below this, there is a search bar with a magnifying glass icon and the text 'Search'. To the right of the search bar is a button labeled 'Quick Assign to All NPIs'. Below the search bar, there are three tabs: 'All (1)', 'Assigned (0)', and 'Unassigned (1)'. The 'All (1)' tab is selected. Below the tabs is a table with the following columns: 'NPI', 'Legal Name', 'Status', and 'Permissions'. The table contains one row with the status 'Unassigned' and a checkbox labeled 'Assign'. At the bottom right of the screen, there are two buttons: 'Skip for now' and 'Next'.

TEST SUB ORG NAME 00045

K
KING, JUSTIN B MD I...

Organization Information: Contact:

Step 1

Assign NPI Permissions

Assign this submitter to NPIs within this organization. All NPIs do not have to be assigned.

Search Quick Assign to All NPIs

All (1) Assigned (0) Unassigned (1)

NPI	Legal Name	Status	Permissions
		Unassigned	<input type="checkbox"/> Assign

Skip for now Next

Figure 2.53: Step 1 Assign NPI Permissions.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

3. Complete **Step 2: Transaction and Claim Type Permissions** by selecting the transactions and claim types for the submitter to grant them access to submit claims on behalf of the organization by selecting Manage or clicking **Manage Selected**. Once complete, click **Next**.

The screenshot shows a two-step process. Step 1, 'Assign NPI Permissions', is marked as 'Complete' with a green checkmark. Step 2, 'Transactions and Claim Type Permissions', is the active step. It includes a search bar, a 'Manage Selected' button, and a table with columns for NPI, Legal Name, Transactions, and Claim Type. A 'Select All' checkbox is checked. The table contains one row with a checked NPI checkbox, 'None' for Transactions and Claim Type, and a 'Manage' link. At the bottom are 'Skip for now' and 'Next' buttons.

Step 1

Assign NPI Permissions

✓ Complete

Step 2

Transactions and Claim Type Permissions

Select transaction and claim types for this submitter's assigned NPIs to give them access to submit on your behalf. You can assign all available transaction and claim types to all NPIs, or customize permissions by NPI. You may only assign transaction and claim types that your organization is eligible for.

Search

Manage Selected

All (1) Assigned (0) Unassigned (1)

✓ Select All

NPI ✓	Legal Name	Transactions	Claim Type
✓		None	None

Manage

Skip for now Next

Figure 2.54: Step 2 Transactions and Claim Type Permissions.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

4. Complete **Step 3: Medi-Cal Telecommunications Provider and Biller Application/Agreement**. Please read the agreement form and then sign with First and Last name along with Title. Once complete, click **Next**.

The screenshot displays the 'Step 3' interface for the 'Medi-Cal Telecommunications Provider and Biller Application/Agreement'. At the top, a dark blue header bar contains the title and a status indicator showing 'McportalB55 Not signed' and 'Not signed'. Below the header, the form is titled 'MEDI-CAL TELECOMMUNICATIONS PROVIDER AND BILLER APPLICATION/AGREEMENT' and includes a note that DHCS and the California MMIS Fiscal Intermediary require a signed form from CMC submitters. The form is divided into several sections: '1.2 BACKGROUND INFORMATION', '2.0 DEFINITIONS', '3.0 CLAIMS ACCEPTANCE AND PROCESSING', and '3.1 CLAIMS CERTIFICATION'. Each section contains detailed text regarding the provider's obligations and the state's policies. At the bottom, there is a checkbox for 'I confirm that I am eligible to sign this agreement on behalf of my organization', followed by input fields for 'First and Last Name' and 'Title'. A signature line is also present, with a note stating 'I, the undersigned, am authorized and do attest and agree to all of the terms and conditions of this agreement.' and a line for 'Electronic Signature:'.

Figure 2.55: Step 3 Medi-Cal Telecommunications Provider and Biller Application/Agreement.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

5. Complete **Step 4: Review and Submit** by reviewing the previous steps. Click **Submit and Approve**.

The screenshot shows a multi-step process interface. The first three steps are completed, each marked with a green checkmark and the word 'Complete'. Step 1 is 'Assign NPI Permissions', Step 2 is 'Transactions and Claim Type Permissions', and Step 3 is 'Medi-Cal Telecommunications Provider and Biller Application/Agreement'. Step 4, 'Review and Submit', is the current active step. It contains a paragraph of text explaining that the signed application will be sent to 'TEST SUB ORG NAME 00045' and that upon receipt, the provider organization will be affiliated to this submitter. At the bottom right of the step 4 section is a blue button labeled 'Submit And Approve'.

Step	Step Name	Status	Action
Step 1	Assign NPI Permissions	Complete	Edit
Step 2	Transactions and Claim Type Permissions	Complete	Edit
Step 3	Medi-Cal Telecommunications Provider and Biller Application/Agreement	Complete	Edit
Step 4	Review and Submit	In Progress	Submit And Approve

Figure 2.56: Step 4 Review and Submit.

6. A notification stating, "Request successfully approved" will appear under the **Pending Requests** tab.

The screenshot shows the 'Pending Requests' tab selected in a navigation bar. Below the navigation bar, a green notification box displays the message 'Request successfully approved'. Below the notification is a table with four columns: 'Organization', 'Date', 'Status', and 'Request Type'. The table is currently empty.

Organization	Date	Status	Request Type
--------------	------	--------	--------------

Figure 2.57: Request successfully approved.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

Deny a Submitter Affiliation Request

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

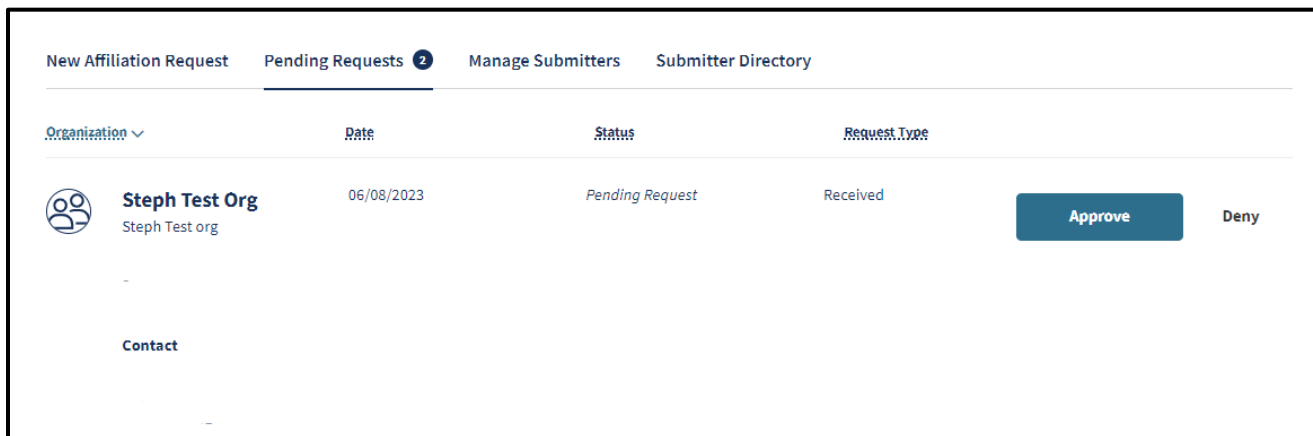


Figure 2.58: Pending Requests.

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

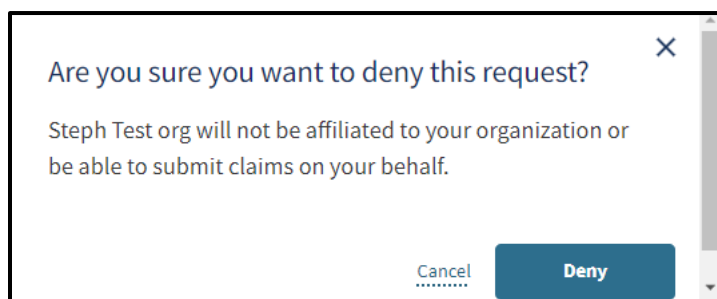


Figure 2.59: Deny Request Confirmation.

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

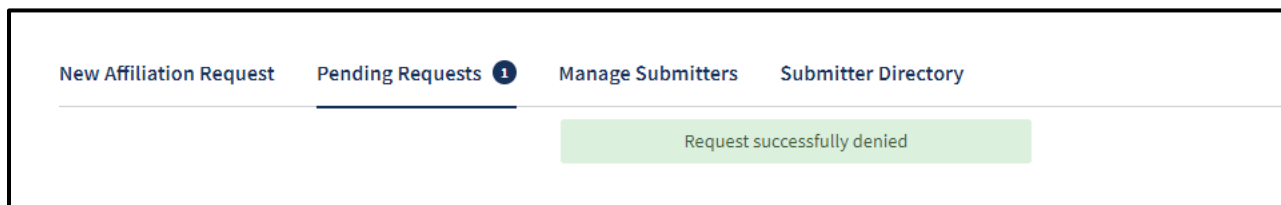


Figure 2.60: Request Successfully Denied.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

Manage Submitters

1. To manage a submitter organization's permissions, select the kebab menu at the end of the row and click **Manage Submitter**.

New Affiliation Request						
Pending Requests 2						
Manage Submitters						
Submitter Directory						
Showing 1-2 of 2						
Organization	Date Approved	Status	NPIs	Transaction	Claim Types	
 Mcportal055	02/07/2024	Active	1770858573	assigned	-----	
 TEST SUB ORG NAME 00045	01/26/2024	Active	1770858573	270,837	medical	

Figure 2.61: Manage Submitters.


Provider Portal User Guide: Provider Organization

Page updated: July 2023

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

Submitter Management and Permissions

Remove submitter from organization

**Mcportal055**
Submitter ID: ABO


Organization Information:

Contact:

Affiliation Status:
Active

Date Approved:
02/07/2024

Last Login Date
02/07/2024

**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 (1)

Assigned (1)

Unassigned (0)

NPI	Legal Name	Status
		Assigned

Figure 2.62: Submitter Management and Permissions.

74

Provider Portal User Guide: Provider Organization

Page updated: July 2023

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

Provider Affiliations

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.

Search

Quick Assign to All NPIs

All (1) Assigned (0) Unassigned (1)

NPI	Legal Name	Status	Permissions
		Unassigned	<input type="checkbox"/> Assign

[Skip for now](#) **Next**

Figure 2.63: Provider Affiliations.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

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

Provider Affiliations

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.

Search

Unassign all NPIs

All (1) Assigned (1) Unassigned (0)

NPI	Legal Name	Status	Permissions
		Assigned	<input checked="" type="checkbox"/> Assign

Skip for now Next

Figure 2.64: Assign NPI Permissions.

- Click **Edit** on the far right of the **Transaction and Claim Type Permissions** area.

Transaction and Claim Type Permissions Edit

Search

All (1) Transaction and Claim Type Permissions Assigned (1) Unassigned (0)

NPI	Legal Name	Transactions	Claim Type
		assigned	None

Figure 2.65: Transaction and Claim Type Permissions.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

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

Transaction and Claim Type Permissions

Select transaction and claim types for this submitter's assigned NPIs to give them access to submit on your behalf. You can assign all available transaction and claim types to all NPIs, or customize permissions by NPI. You may only assign transaction and claim types that your organization is eligible for.

Search Manage Selected

All (1) Transaction and Claim Type Permissions Assigned (1) Unassigned (0)

☐ Select All

NPI	Legal Name	Transactions	Claim Type	
<input type="checkbox"/>		assigned	None	Manage

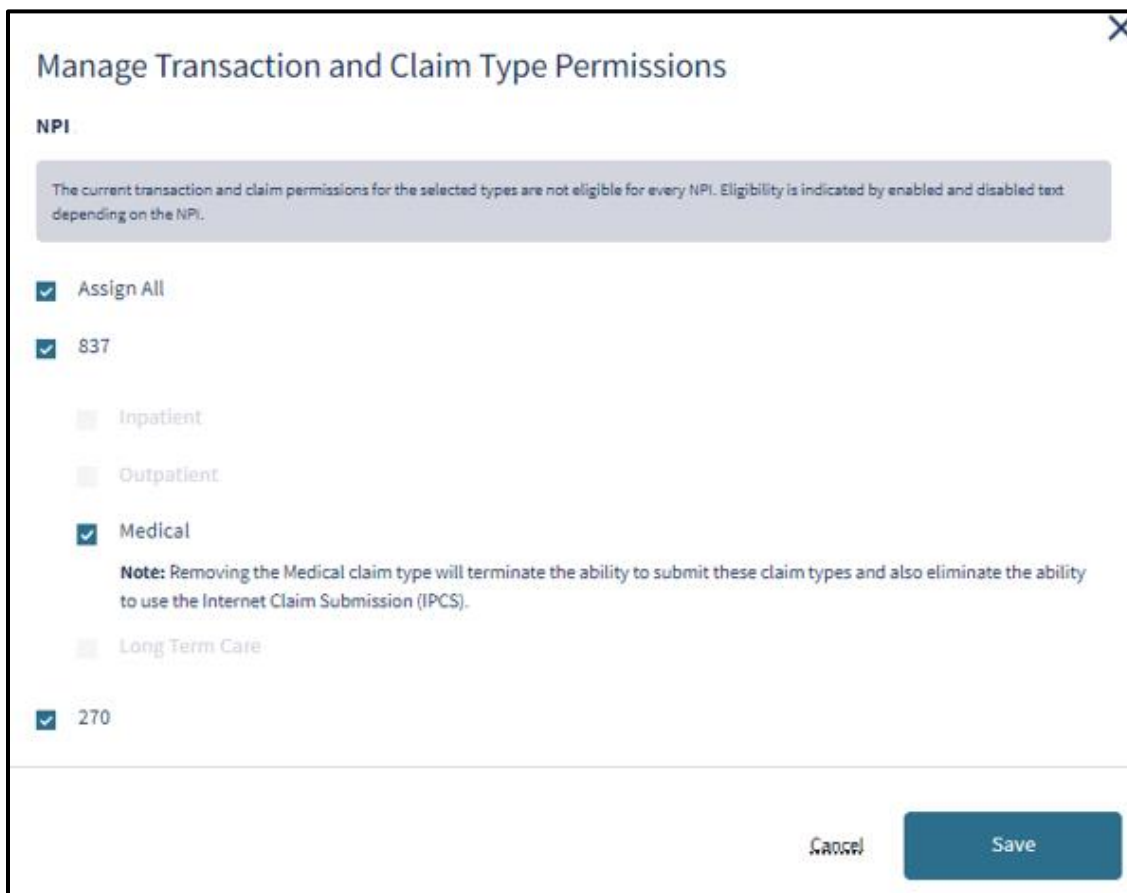
Cancel Next

Figure 2.66: Manage Selected NPIs.

Provider Portal User Guide: Provider Organization

Page updated: July 2023


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



The screenshot shows a modal window titled "Manage Transaction and Claim Type Permissions". At the top, under the "NPI" section, there is a grey informational box stating: "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." Below this, there are several checkboxes for claim types: "Assign All" (checked), "837" (checked), "Inpatient" (disabled), "Outpatient" (disabled), "Medical" (checked), and "Long Term Care" (disabled). A note below the "Medical" checkbox reads: "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)." At the bottom, there is a "270" checkbox (checked). The bottom right corner features a "Cancel" button and a blue "Save" button.

Figure 2.67: 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**.



The screenshot displays a section titled "View Signed Agreement and Signatures". It features a dark blue header bar with the text "Submitter + Provider Affiliation Agreement". To the right of this bar, there are two status indicators: a checkmark next to "Mcpportal055 Signed 02/07/2024" and another checkmark next to "Signed 01/26/2024". Below the header bar, there is a button labeled "View Agreement" with a downward arrow icon.

Figure 2.68: View Signed Agreement and Signatures.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

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.






New Affiliation Request			Pending Requests 2	Manage Submitters	Submitter Directory
			<input type="text" value="Search"/>		
			1 2 3		
Organization ▾	Transaction Types ▾	Contact Information			
 01.DBA.org	None				
 TEST.SUB.ORG.NAME 00046	None				
 TEST.SUB.ORG.NAME 00046	837P (MED) 837I (I/P, O/P, LTC)				
 FRSC	None				
 FRCS	None				

Figure 2.69: Submitter Directory.

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 2.70: NPI Agreements and Settings Tile.

PIN Management

The NPIs that are assigned to an organization are viewable in **PIN Management** on the dashboard. The NPIs available to the user are determined by the user's Administrator. To search NPIs, follow these steps:

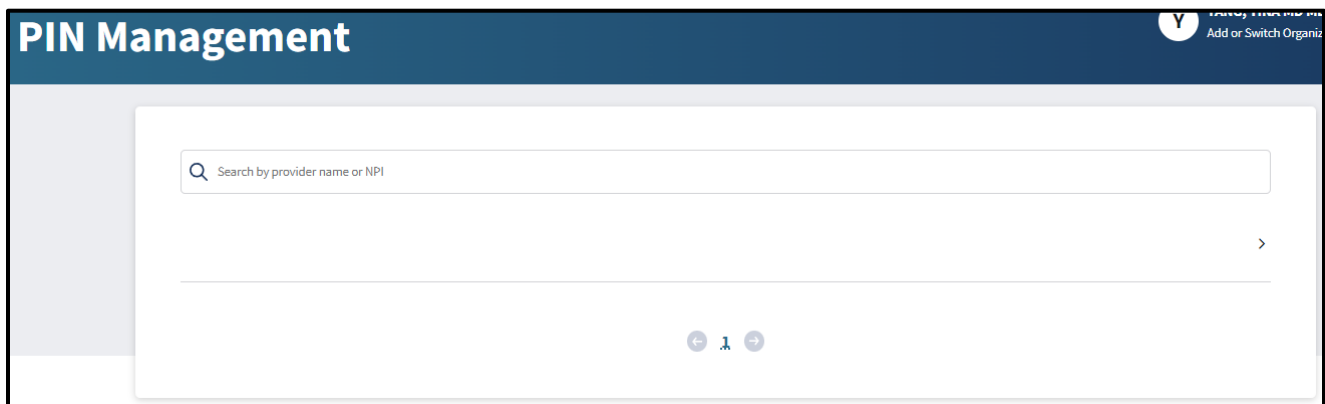


Figure 2.71: PIN Management.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

Reset NPI PIN

To update an NPI PIN, complete the following steps:

1. Click **View All** to see all NPIs. An area to search NPIs appears.

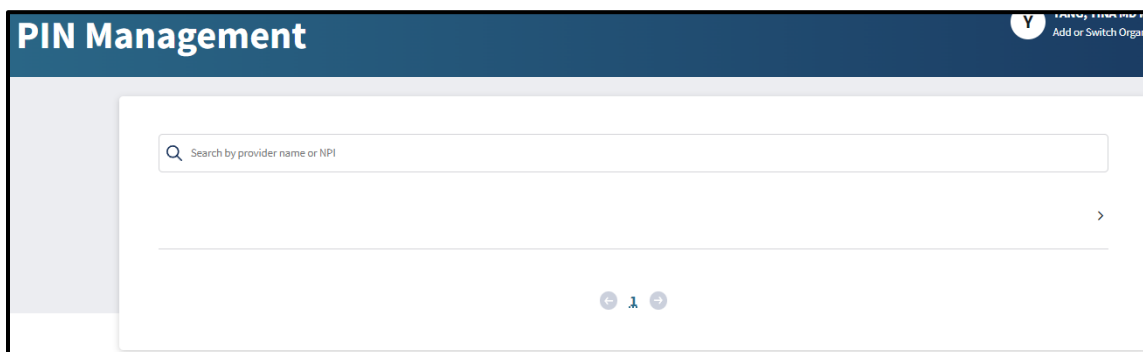


Figure 2.72: Search NPIs.

2. Use the search bar to search for NPI name or number. Select the row for the desired NPI. The NPI profile appears.

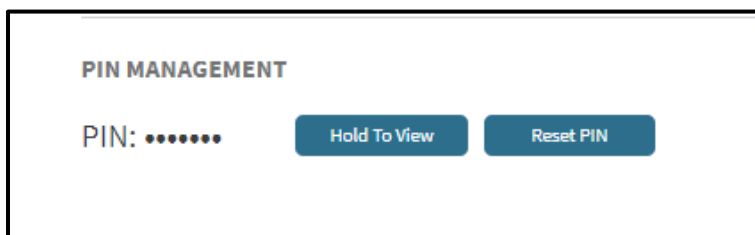


Figure 2.73: Hold to View or Reset PIN.

3. Select **Reset PIN**. The user will be prompted to complete two-factor authentication.
4. Once the user completes the two-factor authentication, a pop-up window appears. Click **Confirm Reset** to reset the PIN. The PIN resets to a randomized 7-digit PIN.

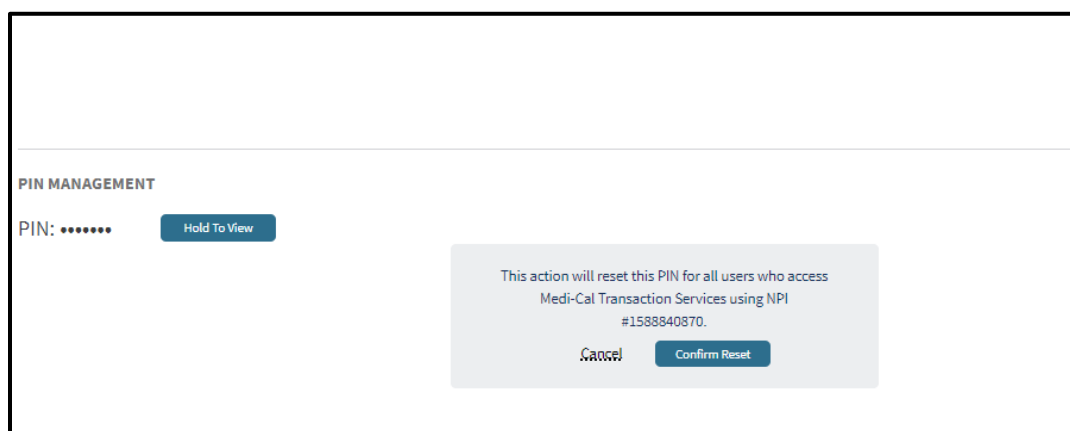


Figure 2.74: Confirm PIN Reset.

Note: The action resets the PIN for all users so be sure to notify any impacted users.

Provider Portal User Guide: Provider Organization

Page updated: May 2024

835 Receiver Management

The **835 Receiver Management** allows organizations to designate up to two entities to receive 835 Transactions. The two receivers can either be an organizational NPI or an affiliated submitter organization. The submitter does not need to be assigned any transaction or claim type privileges to be a designated receiver. The 835 Transaction links will be available for the designated receivers in the Transaction Center.

Add 835 Receiver

1. Click **835 Receiver Management** within the NPI Agreements and Settings tile.



Figure 2.75: NPI Agreements and Settings Tile.

2. A pop-up screen will appear to Complete Receiver Acknowledgement. Click **Go to Receiver Acknowledgement**.

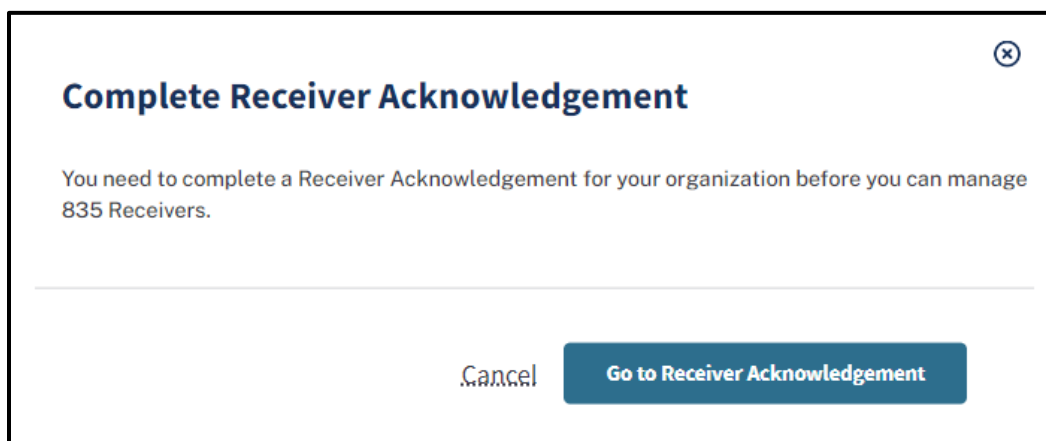
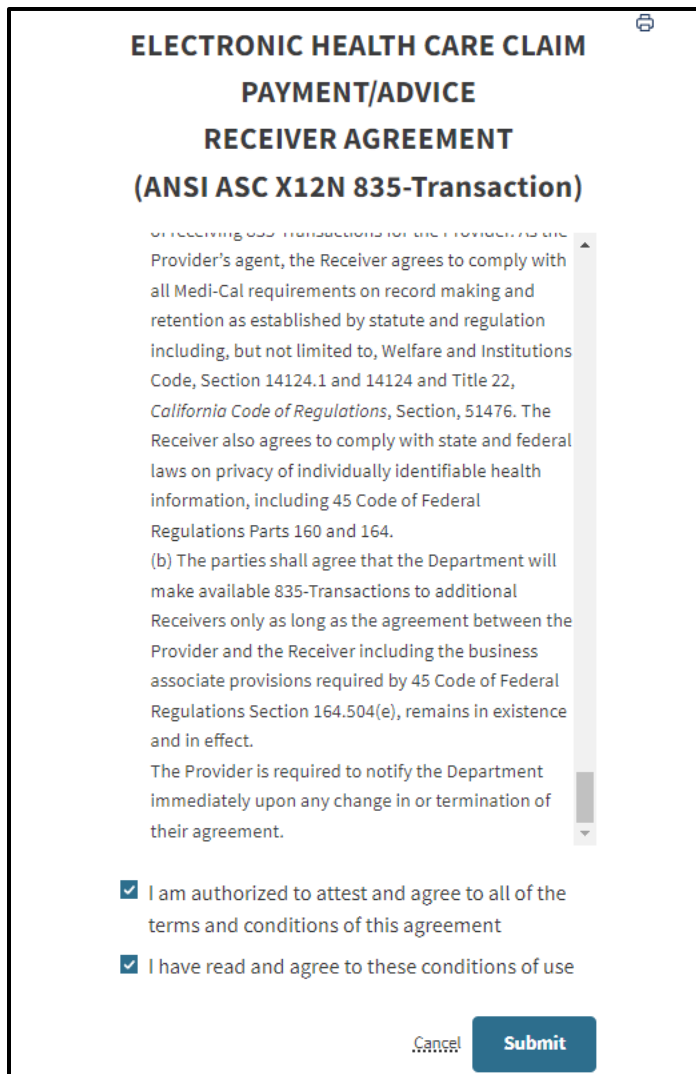


Figure 2.76: Complete Receiver Acknowledgement.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

3. The *Electronic Health Care Payment/Advice Receiver Agreement* (ANSI ASC x12N 835-Transaction) will appear. Read the terms and conditions and select, “I am authorized to attest and agree to all of the terms and conditions of this agreement” and “I have read and agree to these conditions of use.” Click **Submit**.



The screenshot shows a web form titled "ELECTRONIC HEALTH CARE CLAIM PAYMENT/ADVICE RECEIVER AGREEMENT (ANSI ASC X12N 835-Transaction)". The form contains a scrollable text area with the following text: "On receiving 835 transactions for the Provider, as the Provider's agent, the Receiver agrees to comply with all Medi-Cal requirements on record making and retention as established by statute and regulation including, but not limited to, Welfare and Institutions Code, Section 14124.1 and 14124 and Title 22, California Code of Regulations, Section, 51476. The Receiver also agrees to comply with state and federal laws on privacy of individually identifiable health information, including 45 Code of Federal Regulations Parts 160 and 164. (b) The parties shall agree that the Department will make available 835-Transactions to additional Receivers only as long as the agreement between the Provider and the Receiver including the business associate provisions required by 45 Code of Federal Regulations Section 164.504(e), remains in existence and in effect. The Provider is required to notify the Department immediately upon any change in or termination of their agreement." Below the text area are two checkboxes, both of which are checked: "I am authorized to attest and agree to all of the terms and conditions of this agreement" and "I have read and agree to these conditions of use". At the bottom right of the form are two buttons: "Cancel" and "Submit".

**ELECTRONIC HEALTH CARE CLAIM
PAYMENT/ADVICE
RECEIVER AGREEMENT
(ANSI ASC X12N 835-Transaction)**

On receiving 835 transactions for the Provider, as the Provider's agent, the Receiver agrees to comply with all Medi-Cal requirements on record making and retention as established by statute and regulation including, but not limited to, Welfare and Institutions Code, Section 14124.1 and 14124 and Title 22, California Code of Regulations, Section, 51476. The Receiver also agrees to comply with state and federal laws on privacy of individually identifiable health information, including 45 Code of Federal Regulations Parts 160 and 164.

(b) The parties shall agree that the Department will make available 835-Transactions to additional Receivers only as long as the agreement between the Provider and the Receiver including the business associate provisions required by 45 Code of Federal Regulations Section 164.504(e), remains in existence and in effect.

The Provider is required to notify the Department immediately upon any change in or termination of their agreement.

☒ I am authorized to attest and agree to all of the terms and conditions of this agreement

☒ I have read and agree to these conditions of use

[Cancel](#) **Submit**

Figure 2.77: Electronic Health Care Claim Payment/Advice Receiver Agreement (ANSI ASC X12N 835-Transaction).

Provider Portal User Guide: Provider Organization

Page updated: July 2023

4. Click the **add symbol** next to Add Receiver.

835 Receiver Management

An NPI can have a maximum of two receivers. If you wish to add a receiver to an NPI who already has two, then you must remove one first. You can assign two NPIs, two Submitters, or one of each. Use the checkboxes on the right to add the same receiver to multiple NPIs at the same time.

Search by provider name or NPI

NPI Legal Name	Receivers	Select All
	Submitter 001 <input type="checkbox"/>	Submitter ZZH <input type="checkbox"/>
	NPI 0099990422 <input type="checkbox"/>	NPI 0099990444 <input type="checkbox"/>
	Add Receiver <input type="button" value="+"/>	Add Receiver <input type="button" value="+"/>
	Add Receiver <input type="button" value="+"/>	Add Receiver <input type="button" value="+"/>

Figure 2.78: 835 Receiver Management.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

5. Select up to two organizational NPIs or affiliated submitters to be 835 receivers. Once the organizations are selected, click **Confirm** to continue.

Select an 835 Receiver for NPI

Select one organizational NPI or Affiliated Submitter.
If you don't see the Submitter you want, you can make an Affiliation Request.

Organizational NPIs

Search by Provider name or NPI

Affiliated Submitters

Search by Submitter name or ID

ERA TESTING
001

ACS CLEARING HOUSE
ZZZ

ACS 835 TESTING
ZZZ

Cancel Confirm

Figure 2.79: Select an 835 Receiver for NPI.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

6. A pop-up screen will appear asking for confirmation to assign the selected receivers to the NPI. Click **Confirm**.

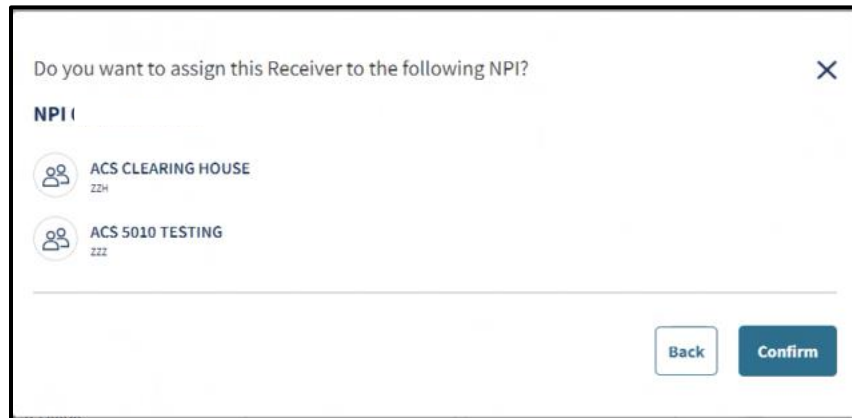


Figure 2.80: Confirmation to Assign Receiver to NPI.

7. Once confirmation is complete, a successfully saved notification will appear and the designated receivers will appear next to the NPI.

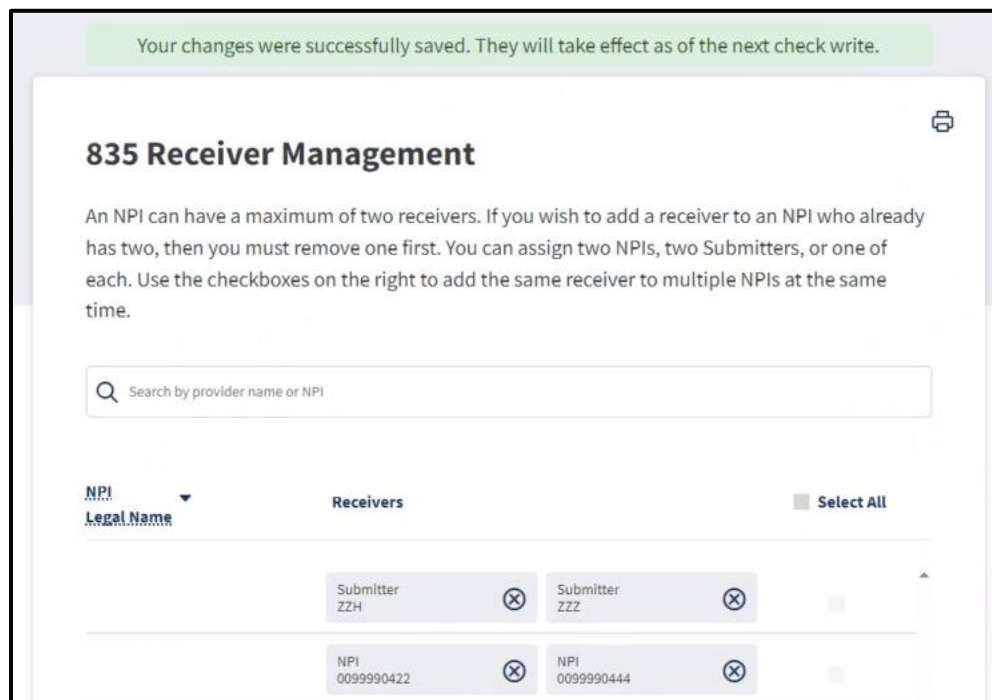


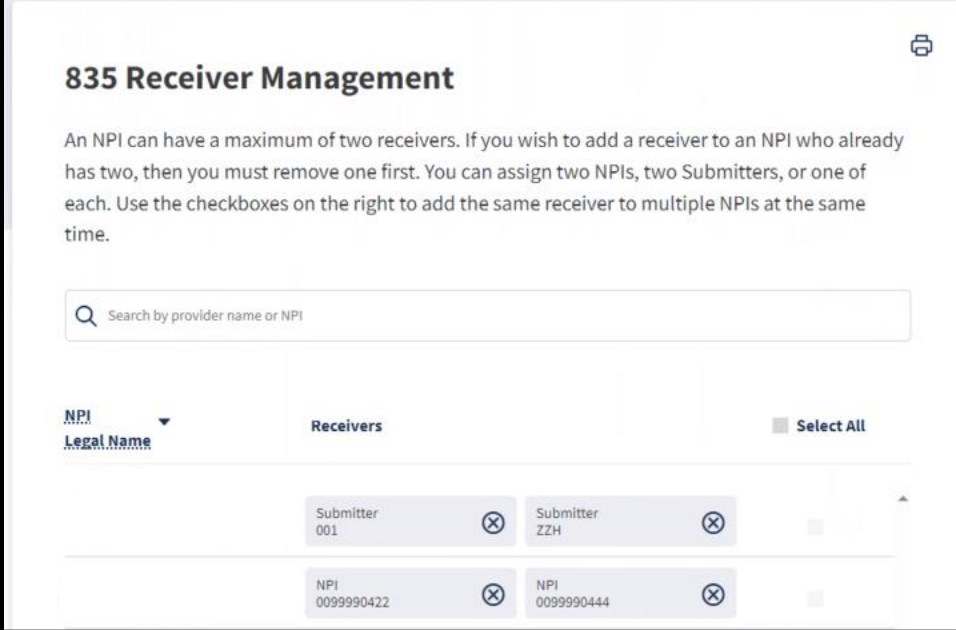
Figure 2.81: Successfully Added Receivers.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

Remove 835 Receiver

1. Click the “x” symbol next to the receiver organization name.



The screenshot shows the "835 Receiver Management" page. At the top, there is a title "835 Receiver Management" and a brief instruction: "An NPI can have a maximum of two receivers. If you wish to add a receiver to an NPI who already has two, then you must remove one first. You can assign two NPIs, two Submitters, or one of each. Use the checkboxes on the right to add the same receiver to multiple NPIs at the same time." Below this is a search bar labeled "Search by provider name or NPI". A table follows with columns for "NPI Legal Name" and "Receivers". The "Receivers" column contains two rows: "Submitter 001" and "Submitter ZZH", each with a checkbox and an "x" icon. Below these are two rows for "NPI 0099990422" and "NPI 0099990444", each with a checkbox and an "x" icon. A "Select All" button is located to the right of the table.

Figure 2.82: 835 Receiver Management.

2. A pop-up screen will appear asking for confirmation to remove the receiver. Click **Remove**.



The screenshot shows a confirmation dialog box titled "Are you sure you want to remove this Receiver?". It contains a user icon and the text "EDS TESTING Submitter EDS TESTING". At the bottom, there are two buttons: "Cancel" and "Remove".

Figure 2.83: Remove Receiver Confirmation.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

3. Once the receiver is removed, a successfully saved notification will appear and the receiver will no longer be listed next to the NPI.

The screenshot displays the '835 Receiver Management' page. At the top, a green notification bar states: 'Your changes were successfully saved. They will take effect as of the next check write.' Below this, the title '835 Receiver Management' is followed by a printer icon. A paragraph explains the rules for adding and removing receivers. A search bar is provided for finding providers by name or NPI. The main section features a table with columns for 'NPI', 'Legal Name', and 'Receivers'. A 'Select All' checkbox is located to the right of the table header. Below the table, there is a 'Submitter' dropdown menu set to 'ZZH' with a removal icon (X), and an 'Add Receiver' button with an addition icon (+).

Your changes were successfully saved. They will take effect as of the next check write.

835 Receiver Management

An NPI can have a maximum of two receivers. If you wish to add a receiver to an NPI who already has two, then you must remove one first. You can assign two NPIs, two Submitters, or one of each. Use the checkboxes on the right to add the same receiver to multiple NPIs at the same time.

Search by provider name or NPI

NPI	Legal Name	Receivers	Select All
-----	------------	-----------	------------

Submitter ZZH [X] Add Receiver [+]

Figure 2.84: Successfully Removed Receiver.

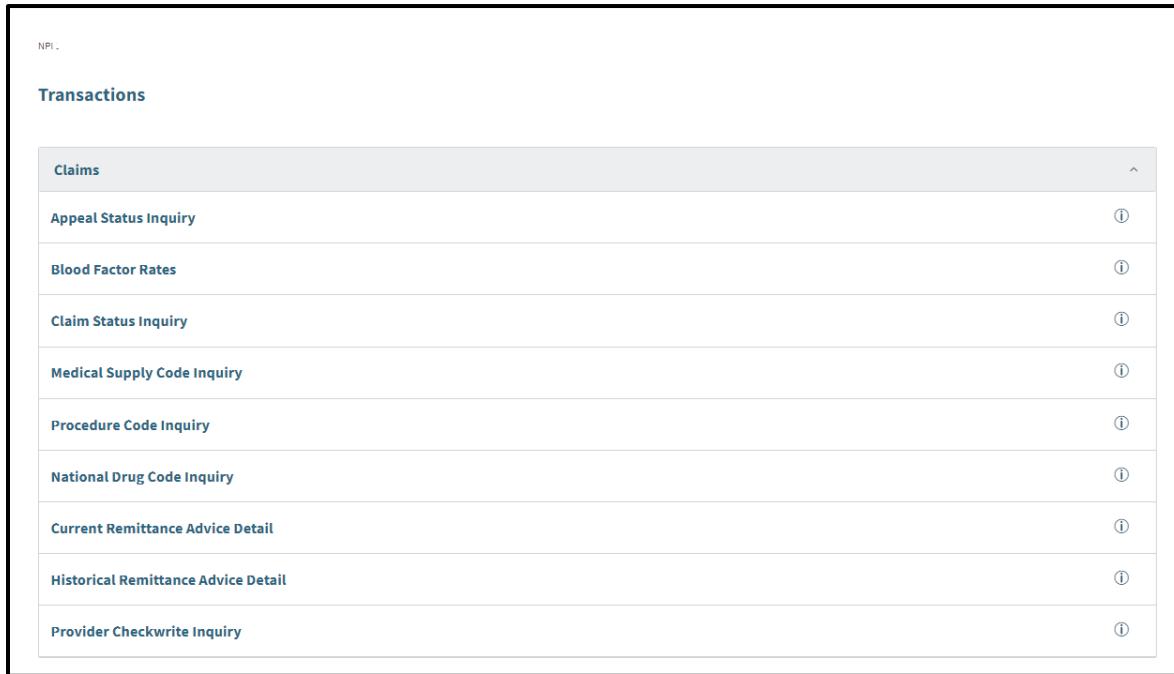
Note: If a submitter removes affiliation from a provider organization, the organization must remove the receiver within 835 Receiver Management.

Provider Portal User Guide: Provider Organization

Page updated: May 2024

Transactions Available

The NPI Transactions that are assigned to an organization can be accessed by the **Transactions Available** link on the dashboard. Once an NPI is assigned by the Organization Administrator, the user will have access to view the available transactions for the designated NPI.



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 2.85: NPI Transactions List.

Provider Portal User Guide: Provider Organization

Page updated: March 2024

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

Figure 2.86: NPI Transactions List.

Provider Portal User Guide: Provider Organization

Page updated: August 2024

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.

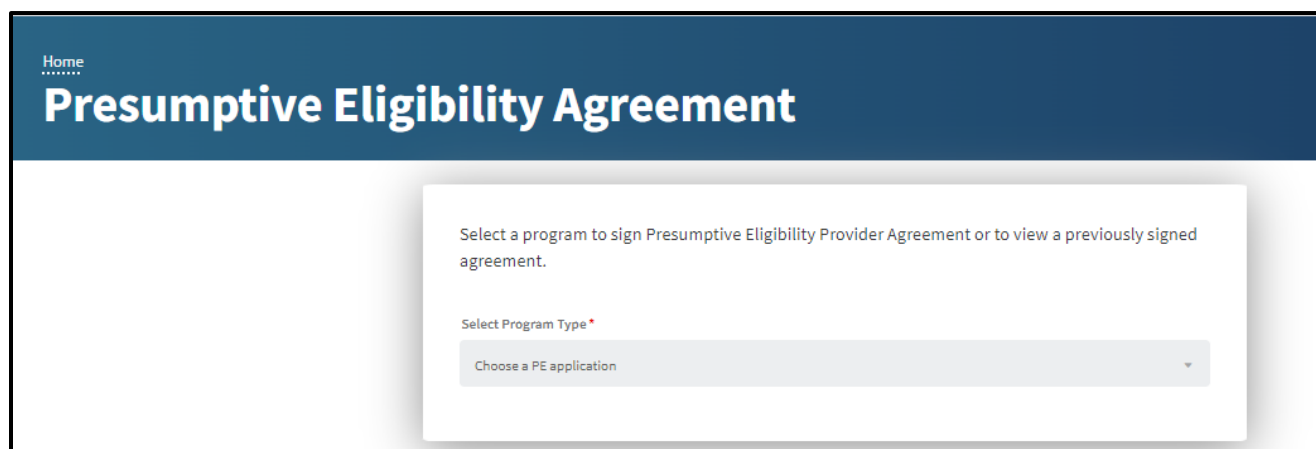


Figure 2.87: Select PE Program Type Drop-Down Menu.

Communication Center

The **Communication Center** allows access to all of an organization's correspondence.

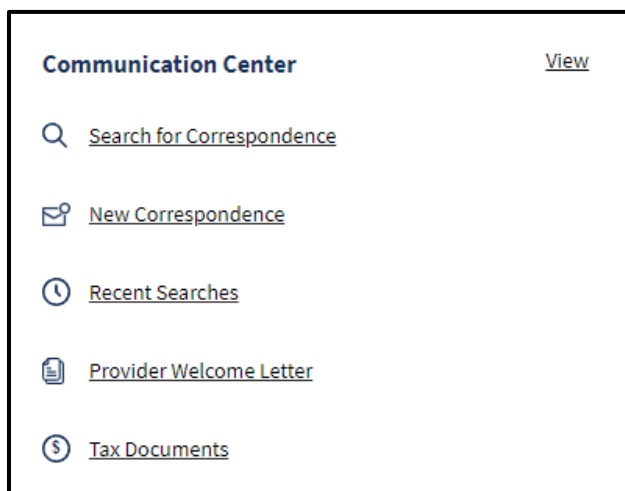


Figure 2.88: Communication Center Tile.

If there is new correspondence, a solid-colored dot appears next to **New Correspondence**.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

Search Correspondence

Complete the following steps to search correspondence:

1. From the **Dashboard**, select **Search for Correspondence**. The Correspondence Center opens.
2. On the left sidebar, select an **NPI** to search for, a **Correspondence Type** and **Dates** to filter through and select **Search**. All three of these search fields must be filled in to get search results.

Note: Only the past six weeks of *Remittance Advice Detail* (RAD) and Supplemental Claims Payment Information (SCPI) are available through the Portal.

The screenshot displays the 'Search for Correspondence' interface. On the left sidebar, there is a search bar with a magnifying glass icon and the text 'Search for Correspondence'. Below this, there are three filter sections: 'NPI' with a dropdown arrow, 'Correspondence Type' with a dropdown menu showing 'PDF Remittance Advice Detail', and 'Dates' with a 'Choose Date Range' dropdown. A blue 'Search' button is positioned below these filters. The sidebar also contains a list of links: 'New Correspondence', 'Recent Searches', 'Provider Welcome Letter', and 'Tax Documents'. The main content area on the right is titled 'Document Results' and shows '0 Documents | Custom'. It features a table with headers 'Name' and 'Date'. A large blue button with the text 'Click filters and search to show documents' is centered in the main area.

Figure 2.89: Search for Correspondence.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

3. To download a single correspondence, select the **three dots** next to the correspondence and click the desired format for the correspondence.

To download more than one correspondence, select the correspondence records and open the **three dots** in the top left corner. The number of selected correspondence records is displayed, and the user may download them using select formats.

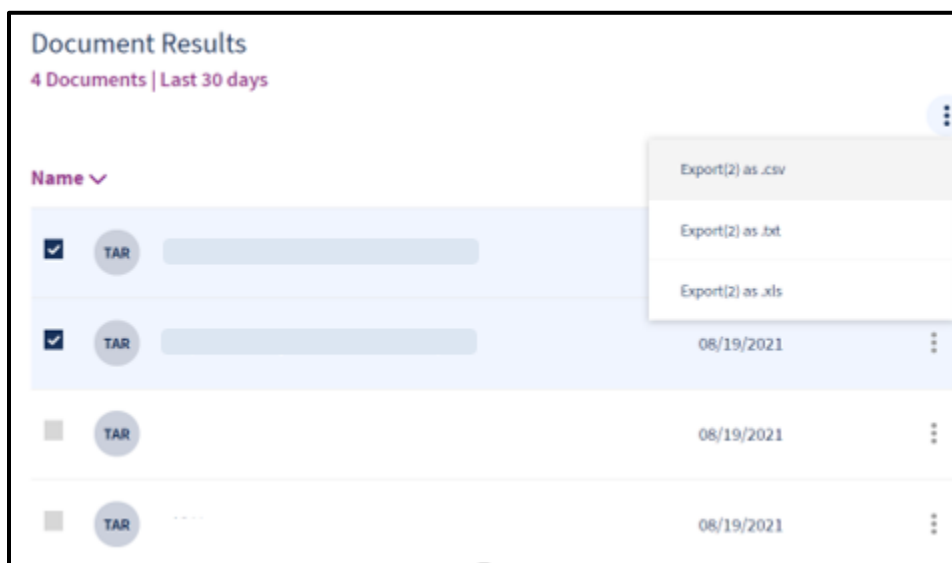


Figure 2.90: Document Results.

4. Click the format to download the correspondence. A pop-up box opens where the user can name the file and choose where to save the file.

View/Download New Correspondence

Complete the following steps to view **new** correspondence:

1. From the dashboard or Communication Center, select **New Correspondence**. The Communication Center opens to the New Correspondence area.
2. New, unread correspondence appears in the right-hand area. To download it, select the **three dots** on the side of the correspondence and select the format for downloading.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

Run Recent Searches

The Communication Center saves the most recent correspondence searches, making it simple to rerun a search if needed. To rerun a search, complete the following steps:

1. From the **Dashboard** or **Communication Center**, click **Recent Searches**. The Communication Center opens and recent searches display.

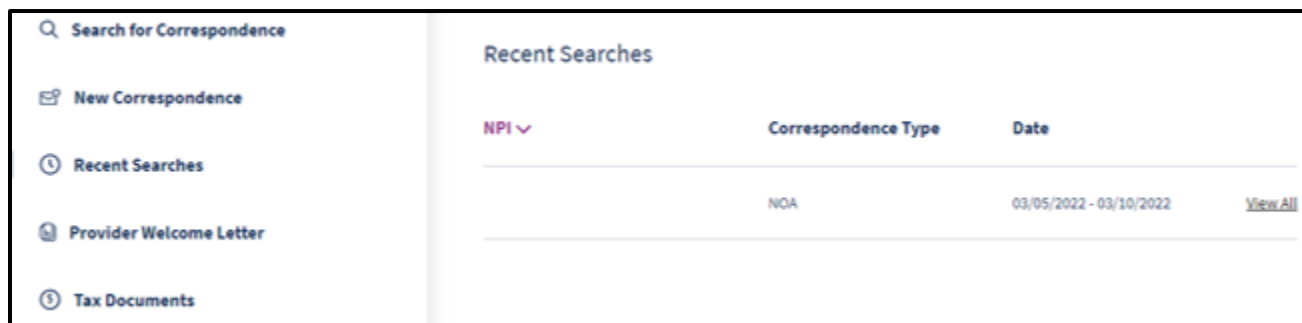


Figure 2.91: Search for Correspondence.

2. To rerun the search, click **View All**. All correspondence that matches the search appear.

View Provider Welcome Letters

Provider welcome letters contain information about NPIs, and provider communities related to the organization. To view, complete the following steps:

1. From the **Dashboard** or **Communication Center**, select **Provider Welcome Letter**. The Communication Center opens to the Provider Welcome Letter page. Click the provider type.

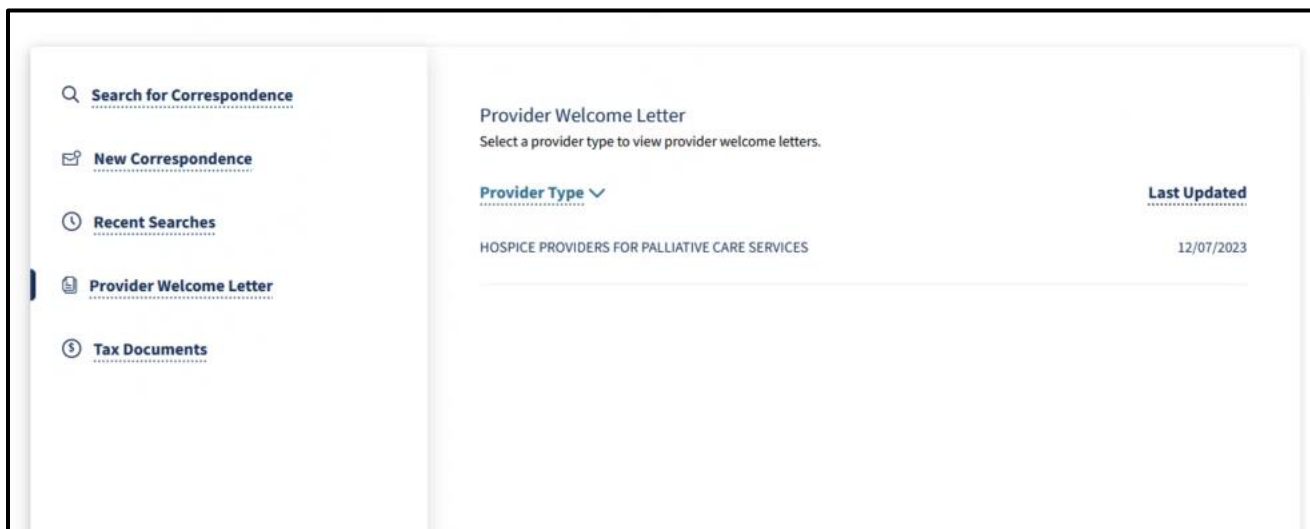
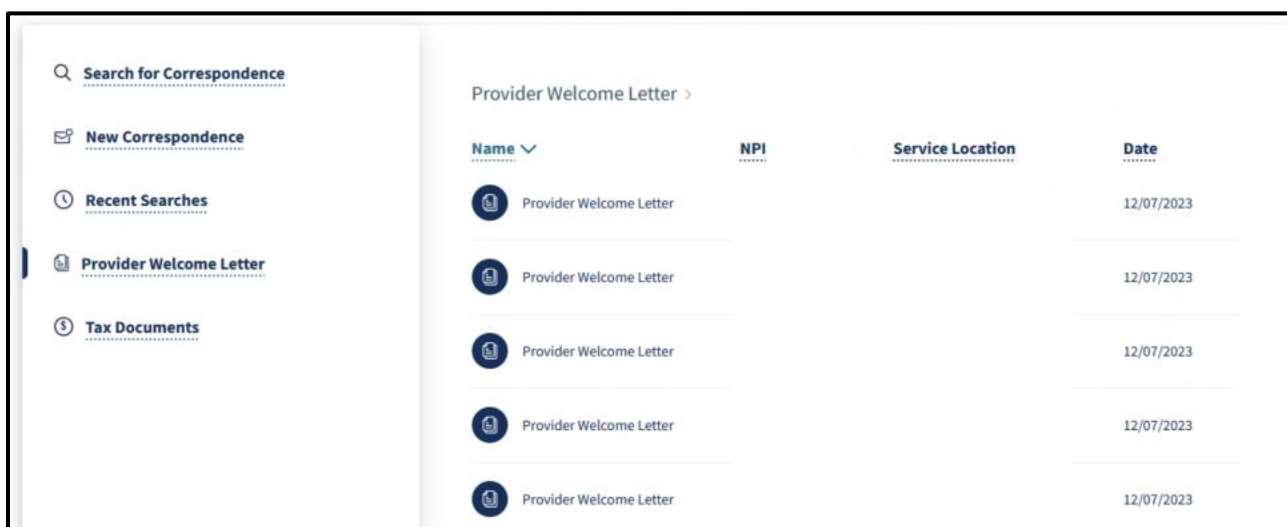


Figure 2.92: Provider Welcome Letter.

Provider Portal User Guide: Provider Organization

Page updated: July 2023

2. Provider letters for NPIs assigned to that provider community appear. Click the desired letter.



The screenshot shows a web application interface. On the left is a sidebar with navigation links: 'Search for Correspondence', 'New Correspondence', 'Recent Searches', 'Provider Welcome Letter' (which is highlighted with a blue bar), and 'Tax Documents'. The main content area is titled 'Provider Welcome Letter >'. It contains a table with four columns: 'Name', 'NPI', 'Service Location', and 'Date'. There are five rows, each representing a 'Provider Welcome Letter' dated '12/07/2023'. Each row has a document icon to the left of the 'Name' column.

Name	NPI	Service Location	Date
Provider Welcome Letter			12/07/2023
Provider Welcome Letter			12/07/2023
Provider Welcome Letter			12/07/2023
Provider Welcome Letter			12/07/2023
Provider Welcome Letter			12/07/2023

Figure 2.93: List of Provider Welcome Letters.

3. A PDF version of the letter appears.

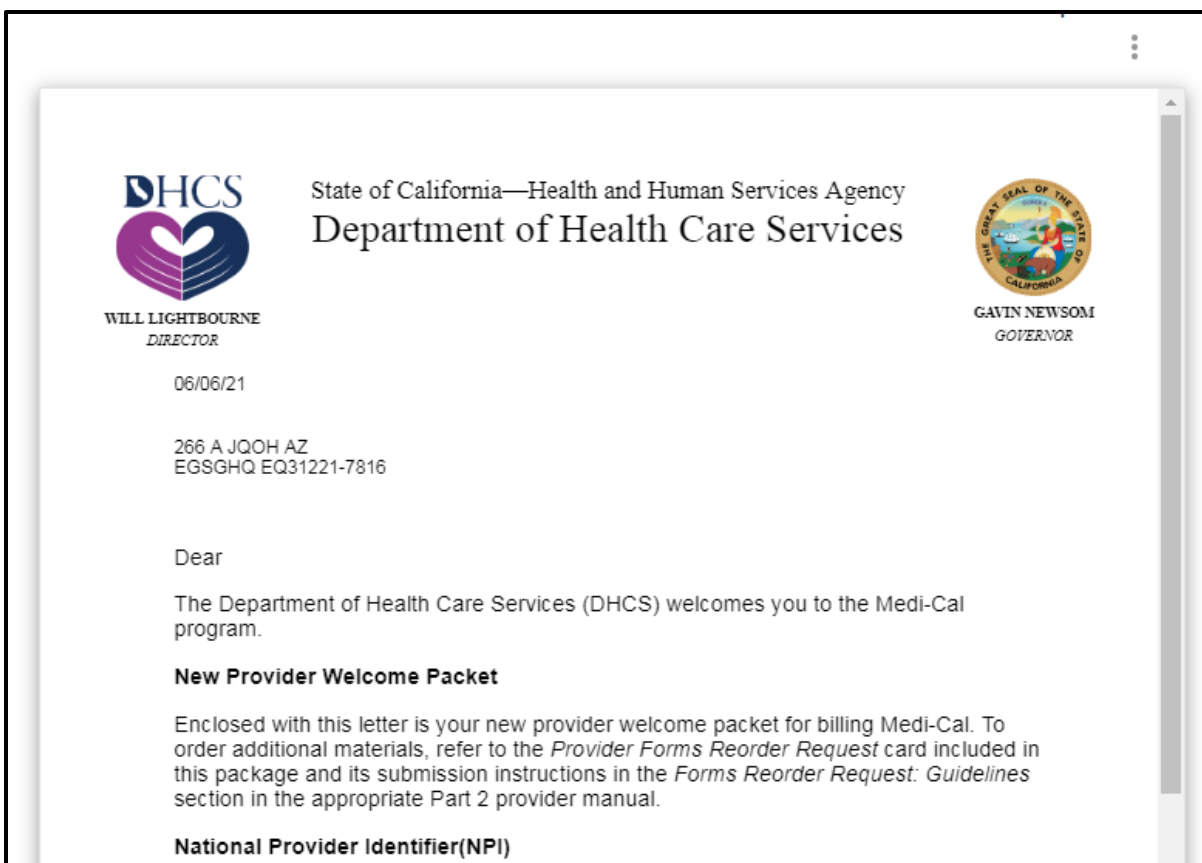


Figure 2.94: Provider Welcome Letter PDF.

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.