State of California
Department of Health Care Services

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

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**.

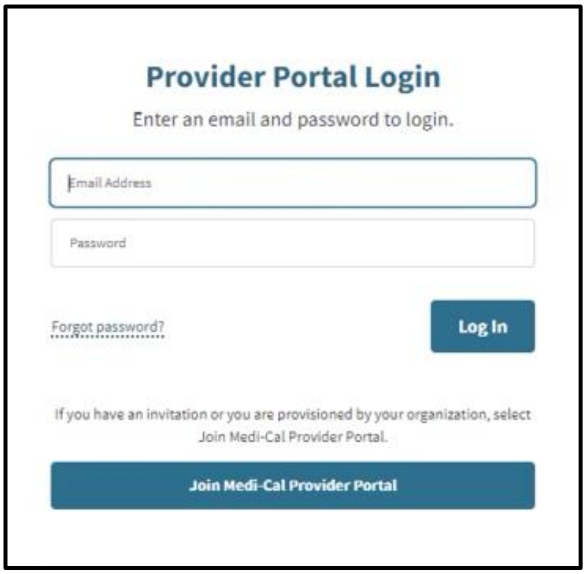


Figure 1.1: Join Medi-Cal Provider Portal Log In.

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

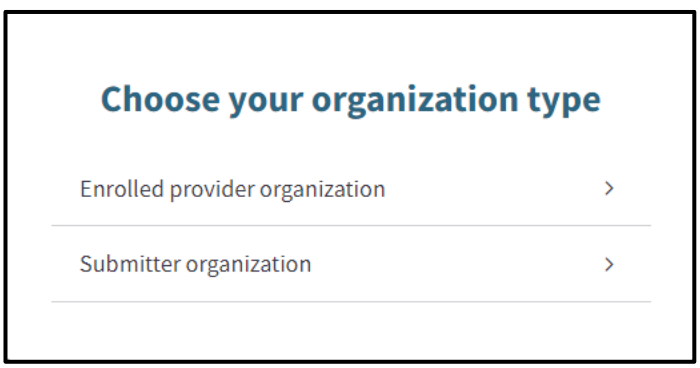


Figure 1.2: Choose your organization type.

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

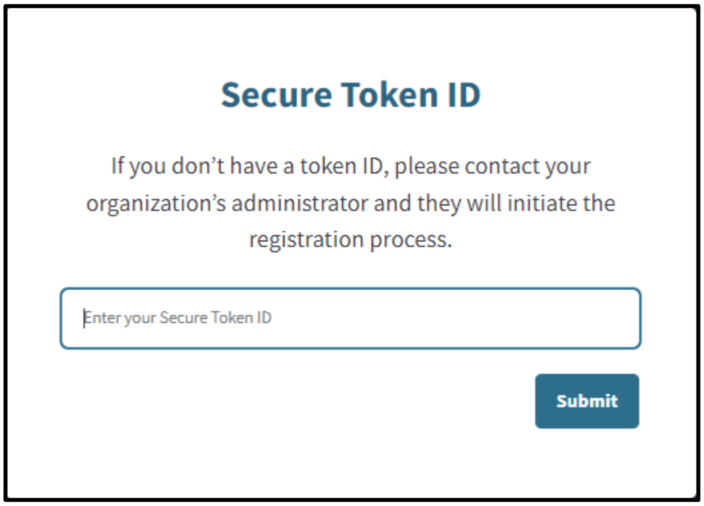


Figure 1.3: Secure Token ID.

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

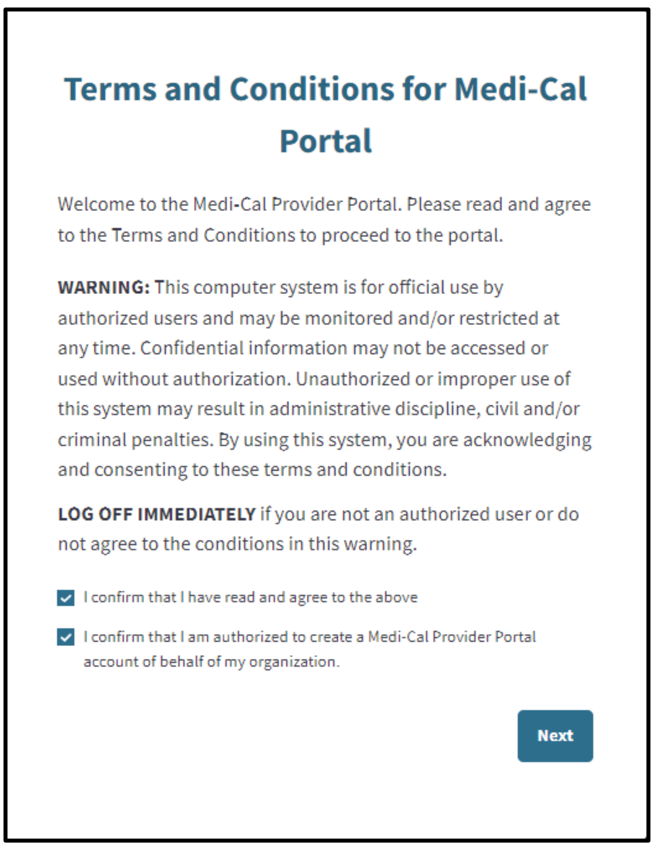


Figure 1.4: Terms and Conditions for Medi-Cal Portal.

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**.

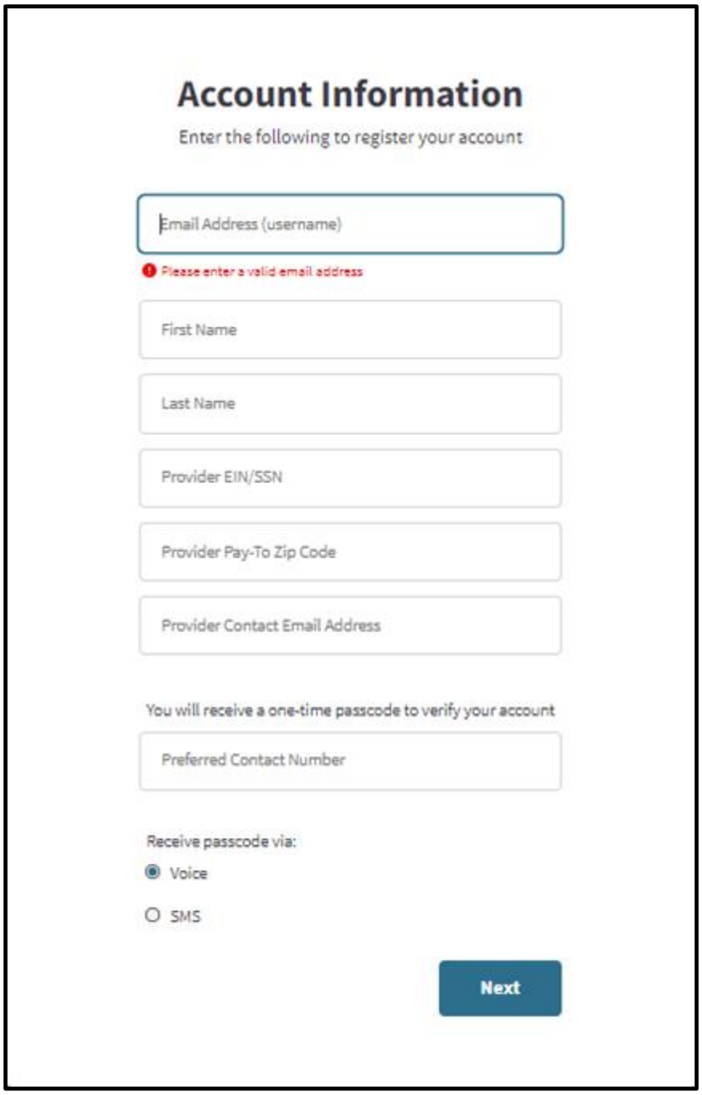


Figure 1.5: Account Information.

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

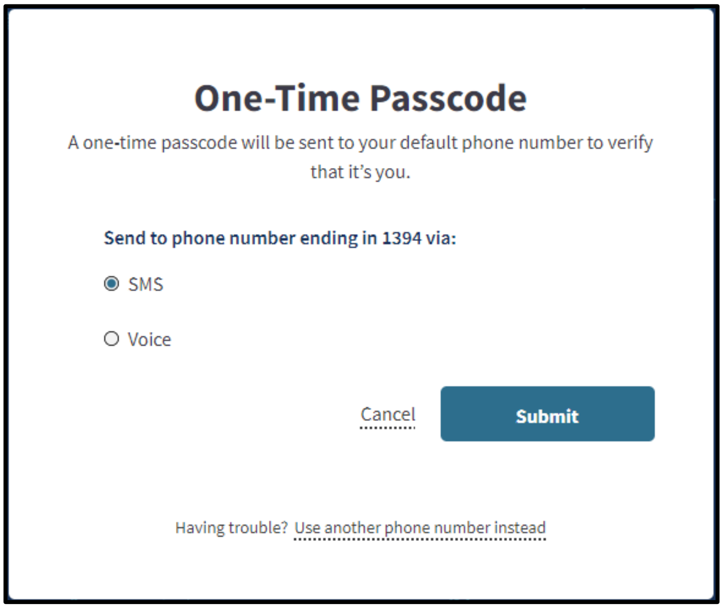


Figure 1.6: One-Time Passcode.

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**.

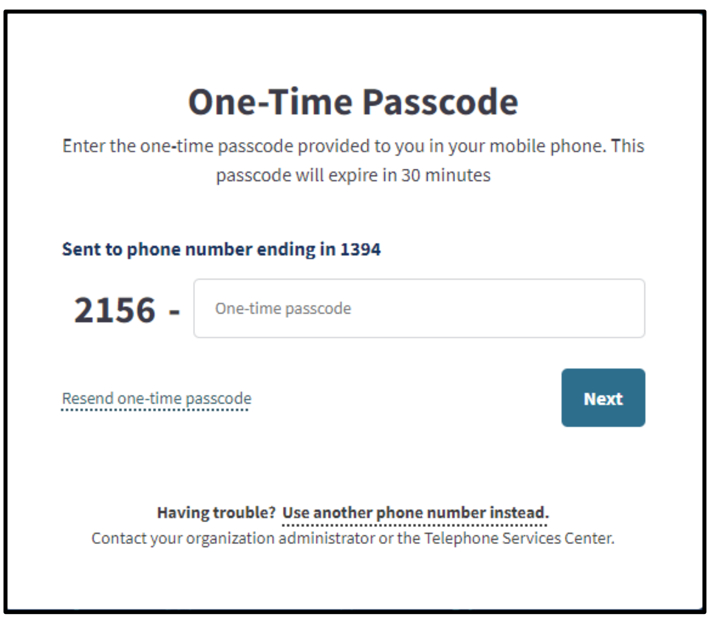


Figure 1.8: Enter One-Time Passcode.

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

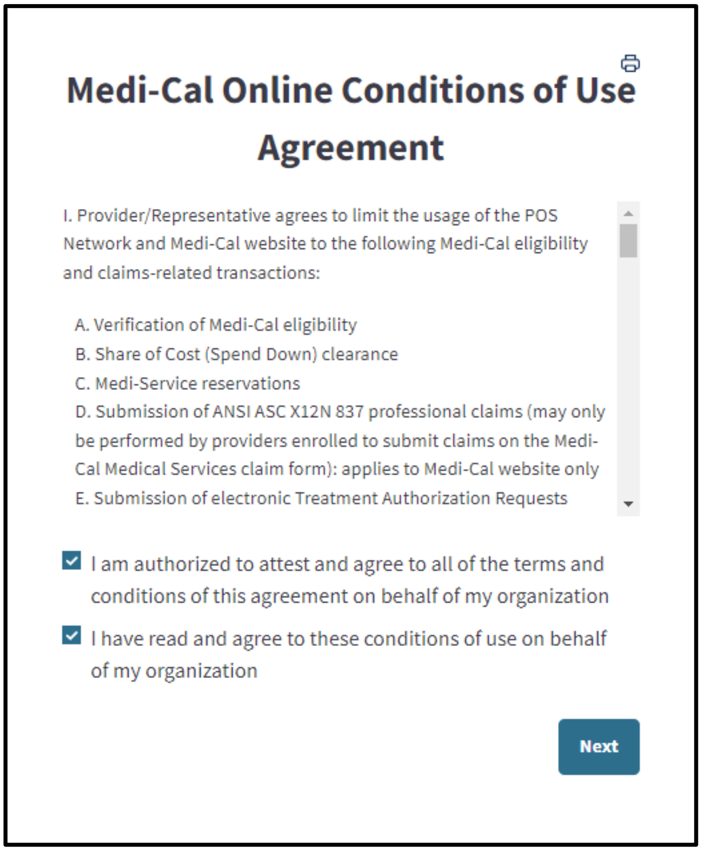


Figure 1.9: Medi-Cal Online Conditions of Use Agreement.

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.

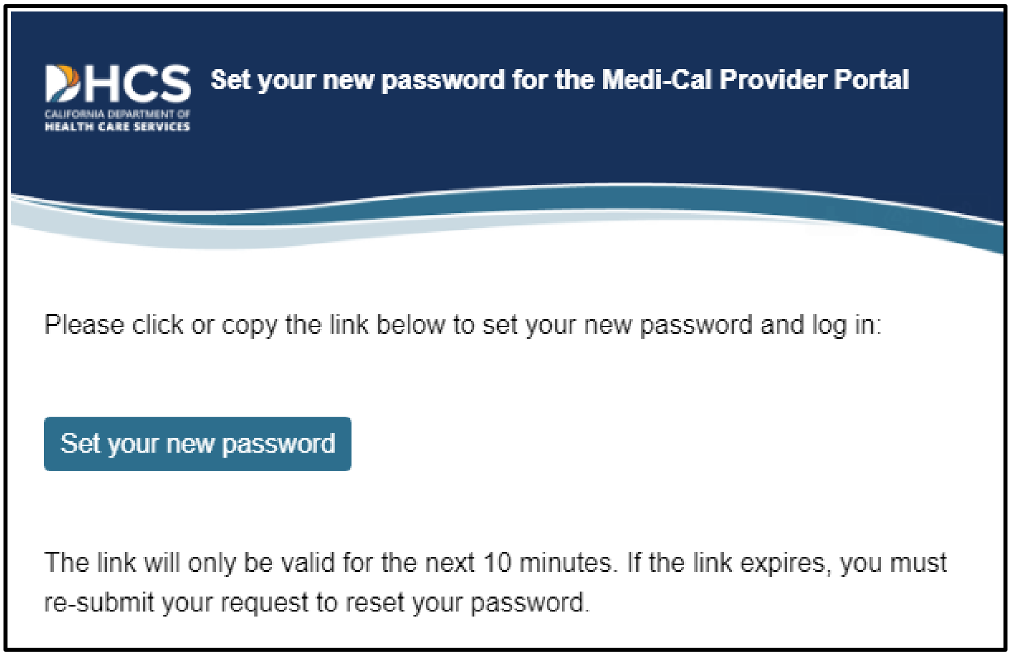


Figure 1.10: Set new password email notification.

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

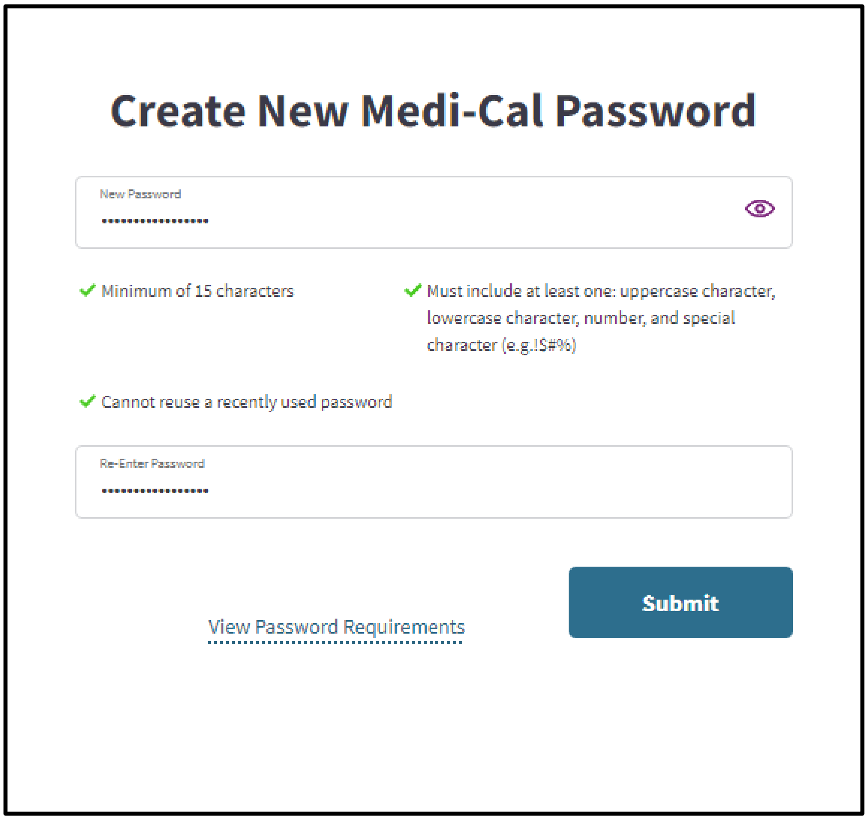


Figure 1.11: Create New Medi-Cal Password.

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.

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.

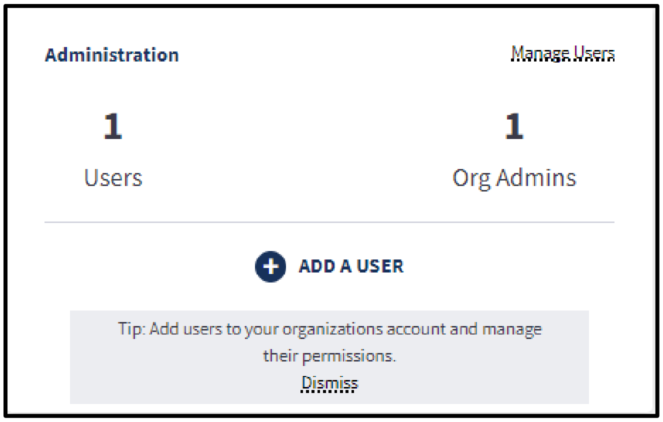


Figure 1.12: Administration Tile.

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.

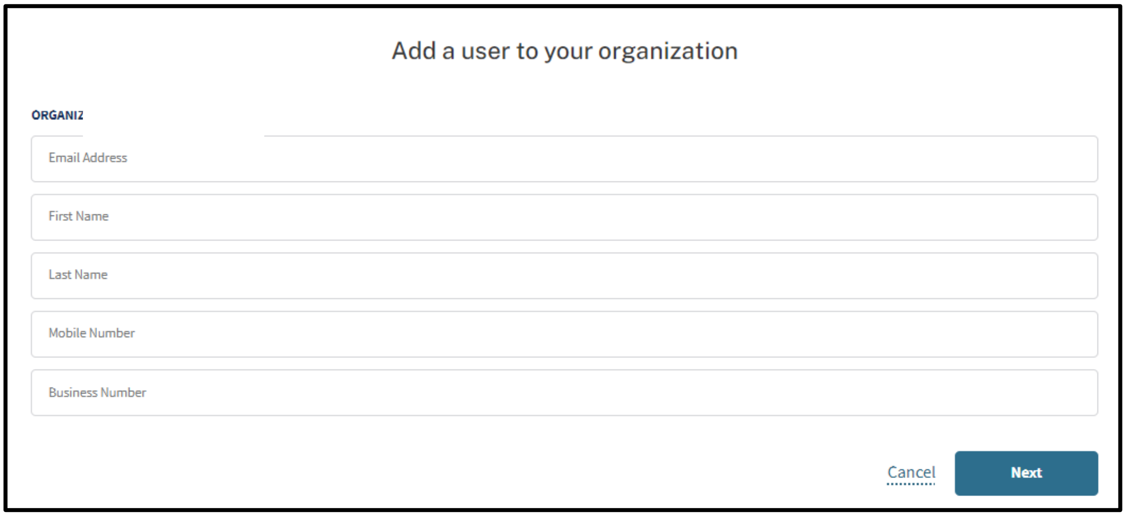


Figure 1.13: Add a User.

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.**

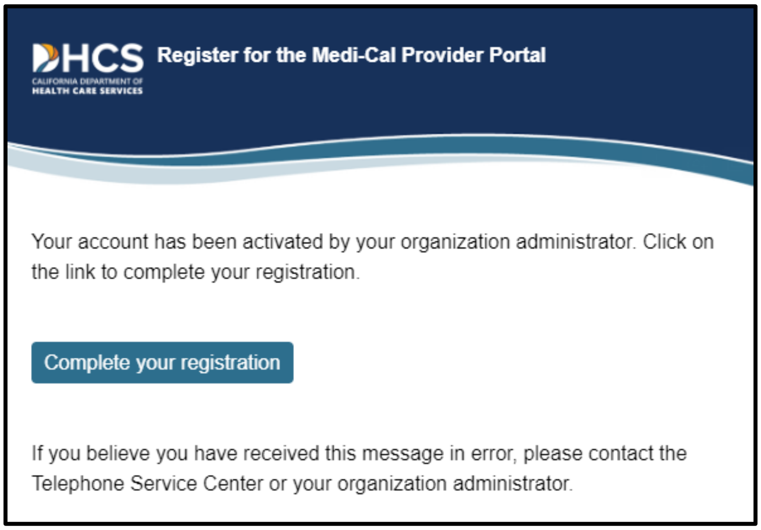


Figure 1.14: Register for the Medi-Cal Provider Portal email notification.

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

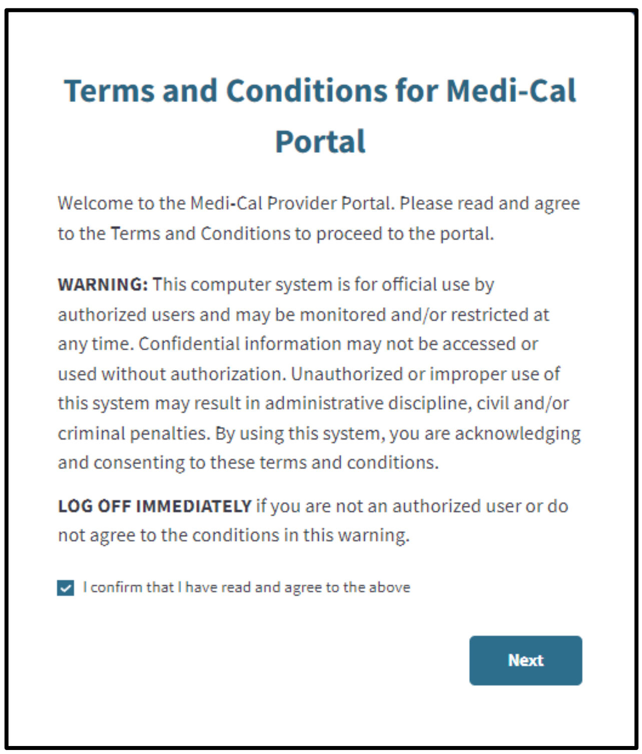


Figure 1.15: Terms and Conditions for Medi-Cal Portal.

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**.

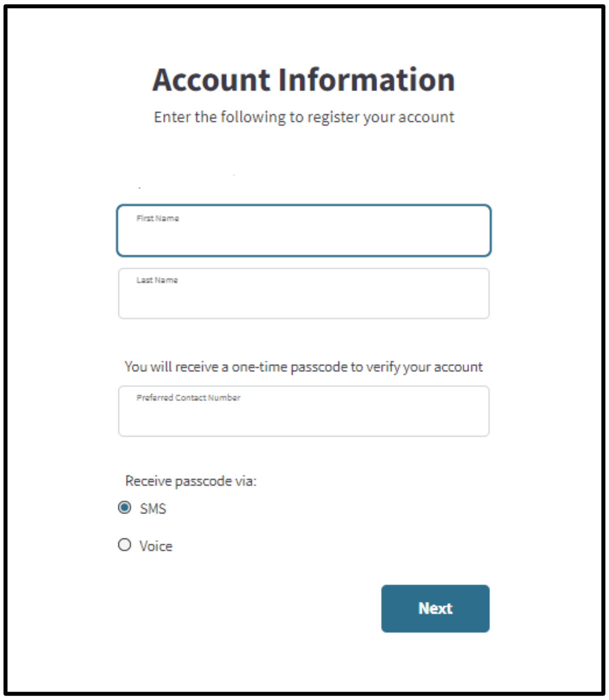


Figure 1.16: Account Information.

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.**

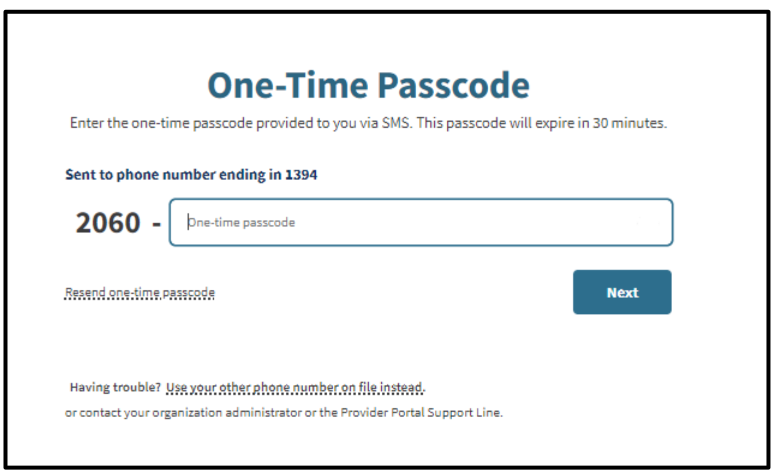


Figure 1.17: Enter One-Time Passcode.

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**.

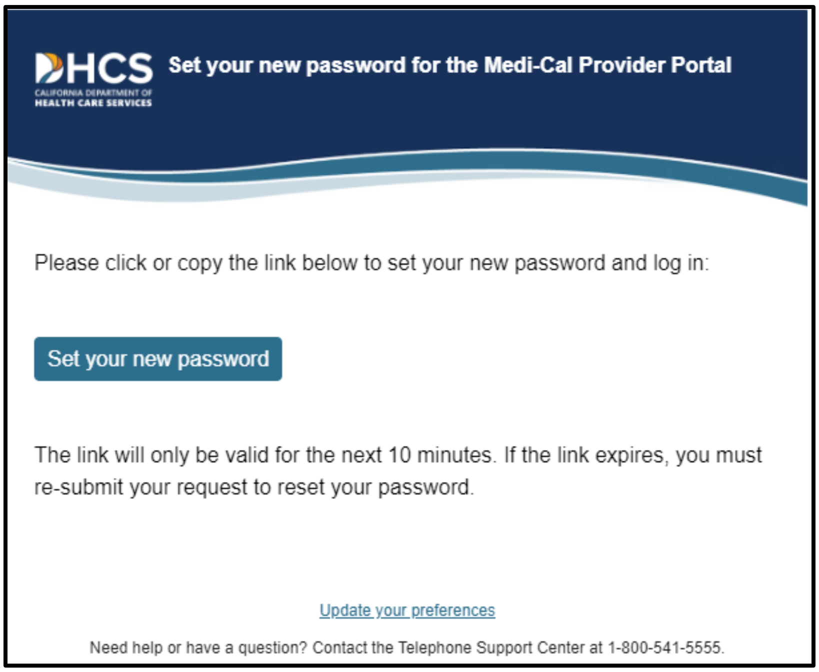


Figure 1.19: Set new password email notification.

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.

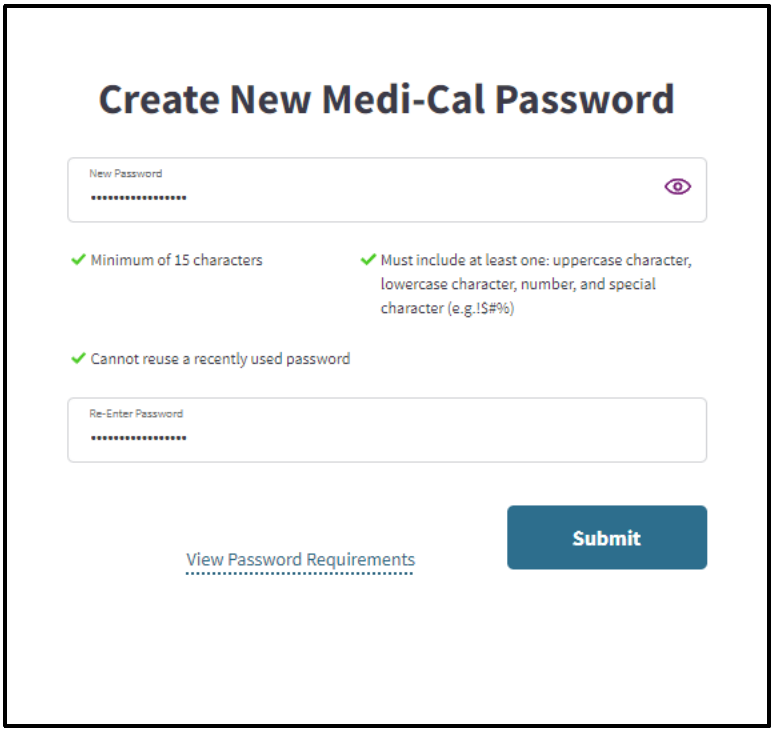


Figure 1.20: Create New Medi-Cal Password.

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.

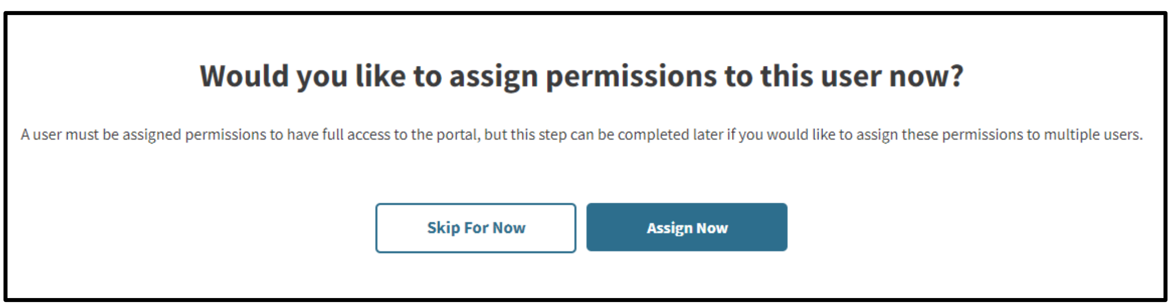


Figure 1.21: Assign User Permissions.

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.

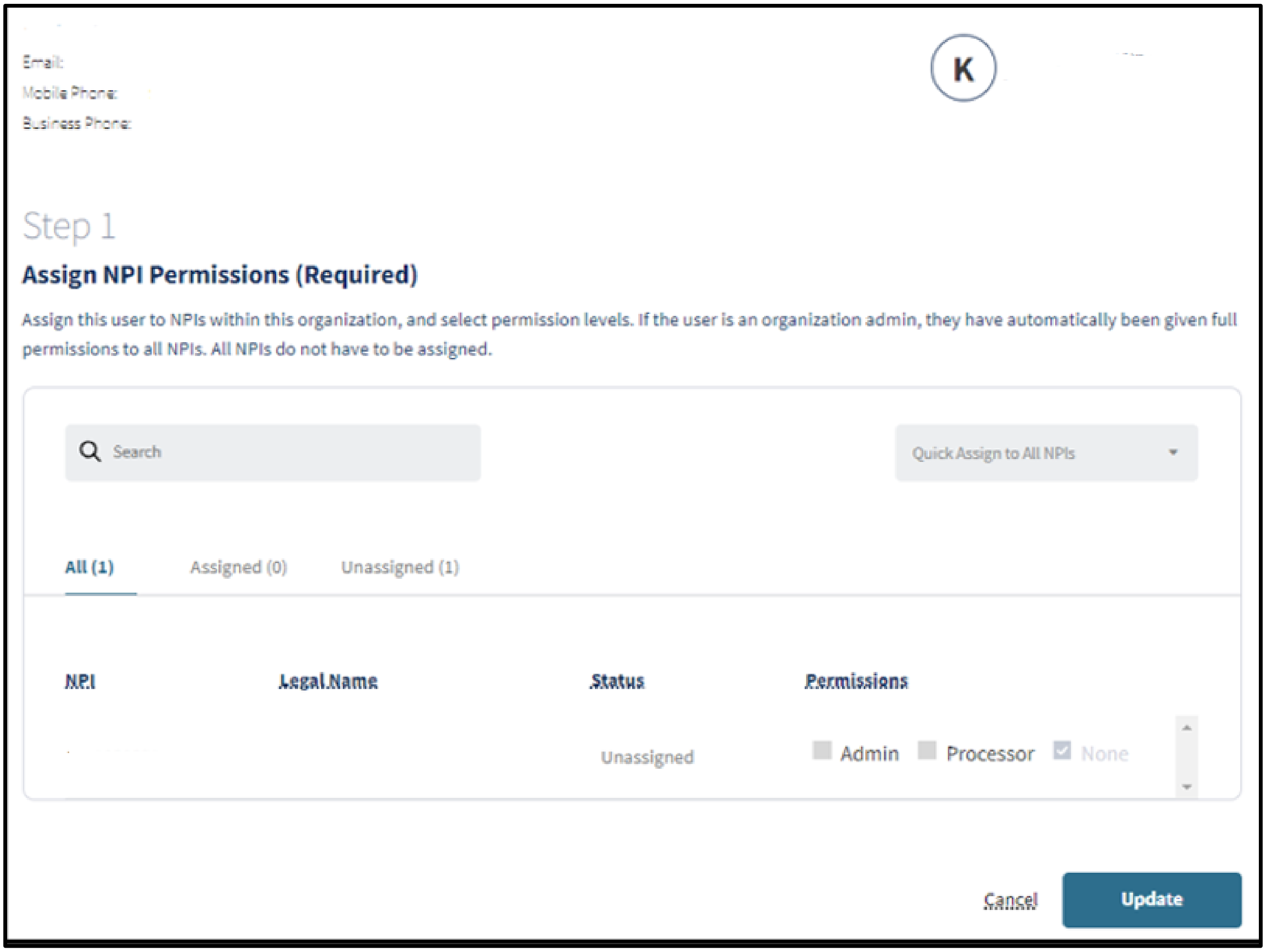


Figure 1.22: Assign NPI Permissions.

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

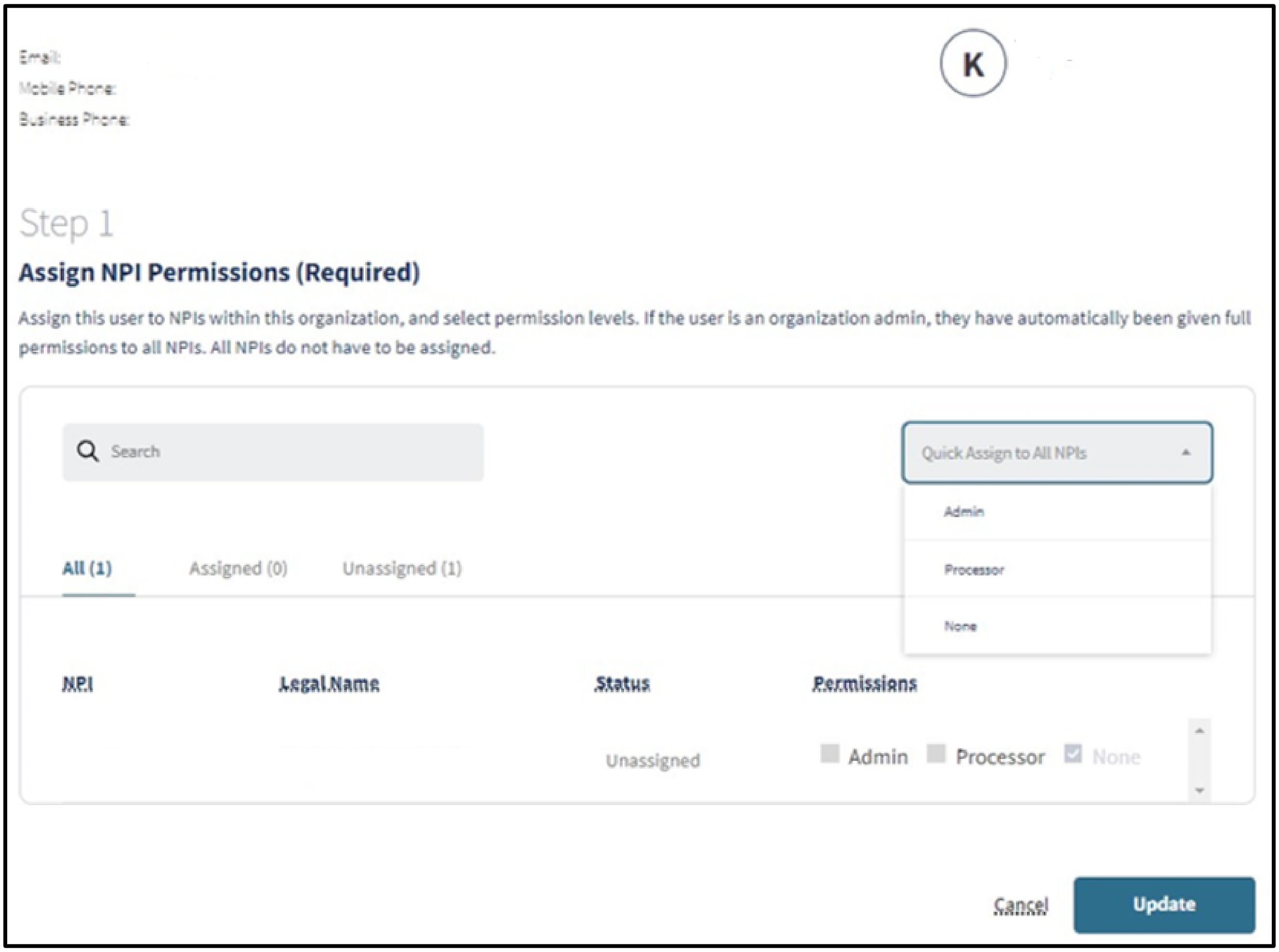


Figure 1.23: Step 1 Quick Assign to All NPIs.

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

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.

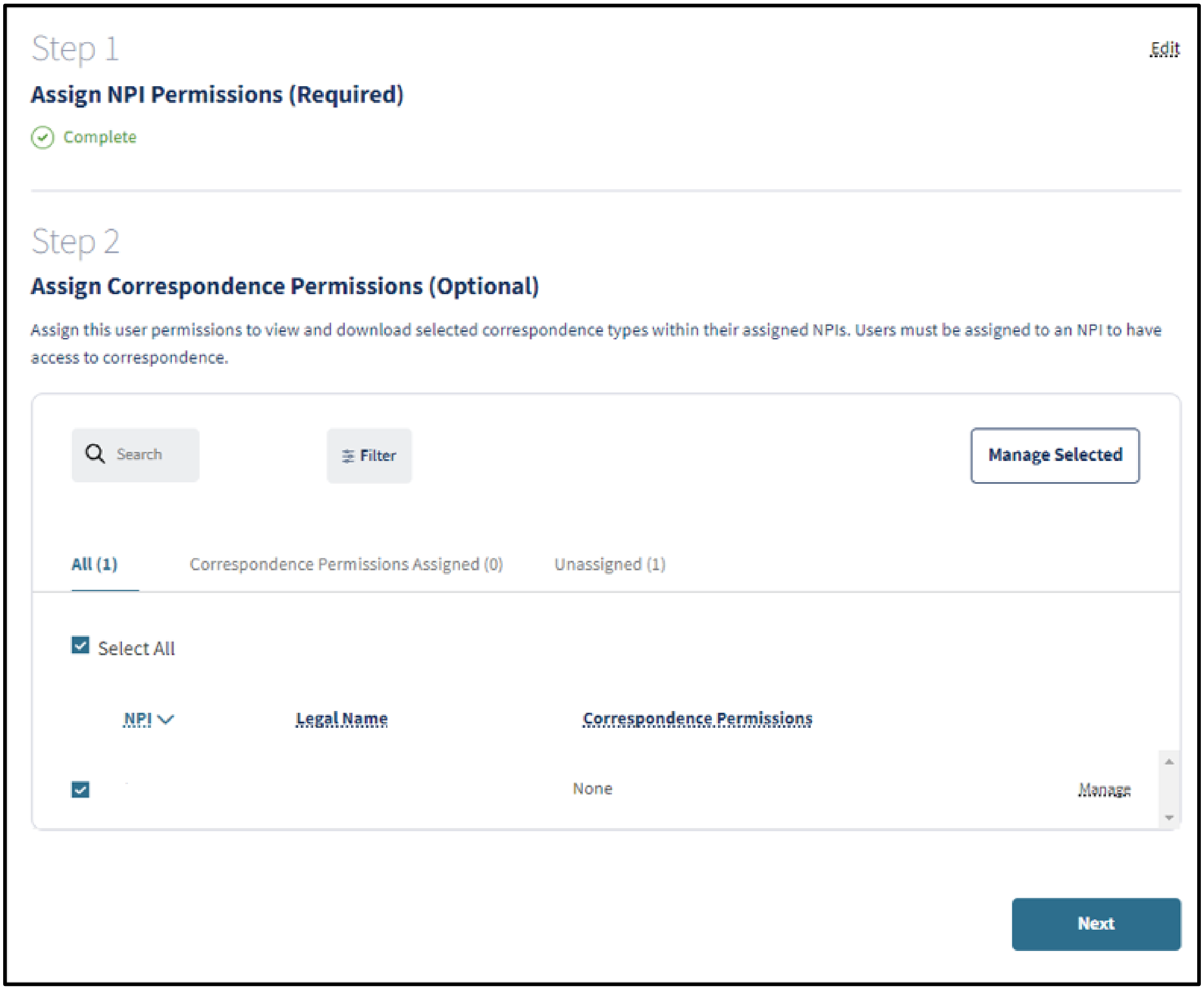


Figure 1.24: Step 2 Assign Correspondence Permissions.

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

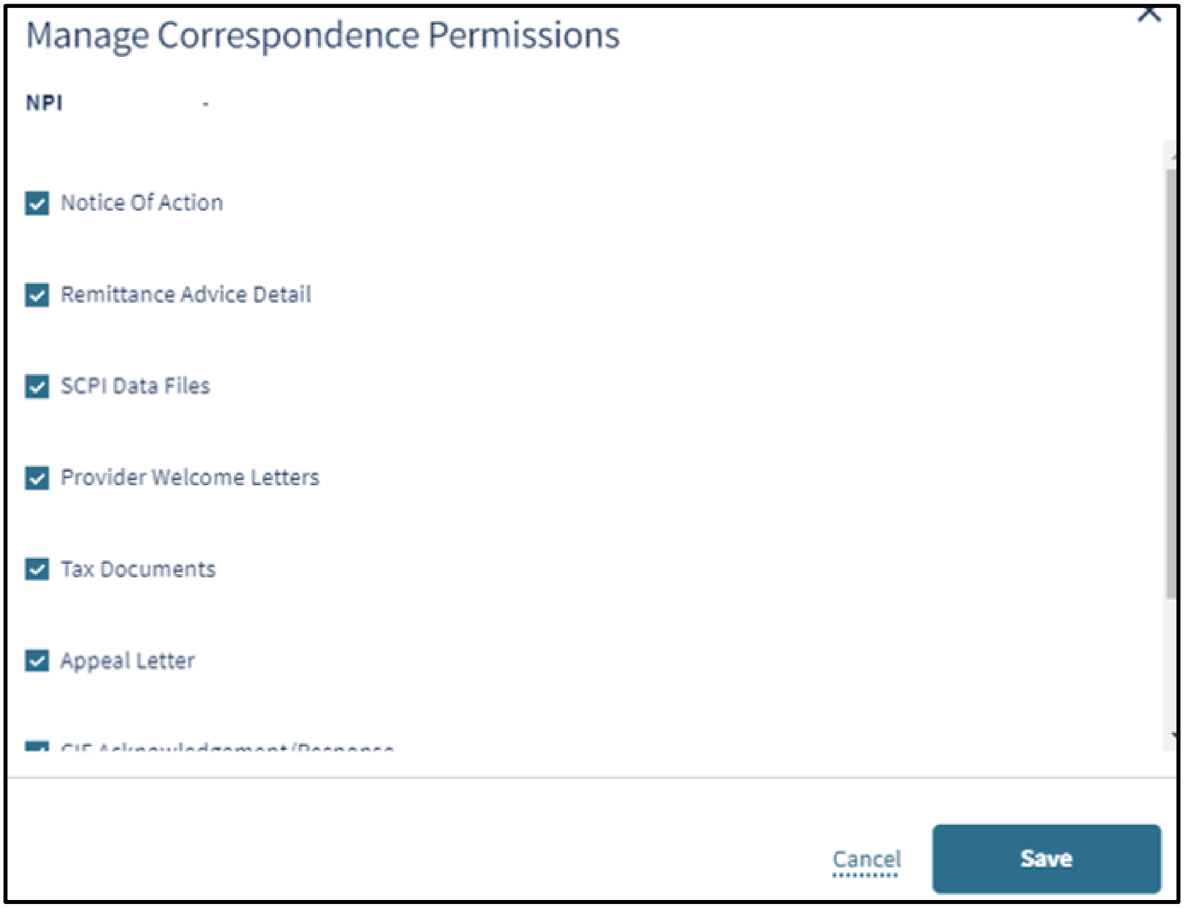


Figure 1.25: Manage Correspondence Permissions.

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**.

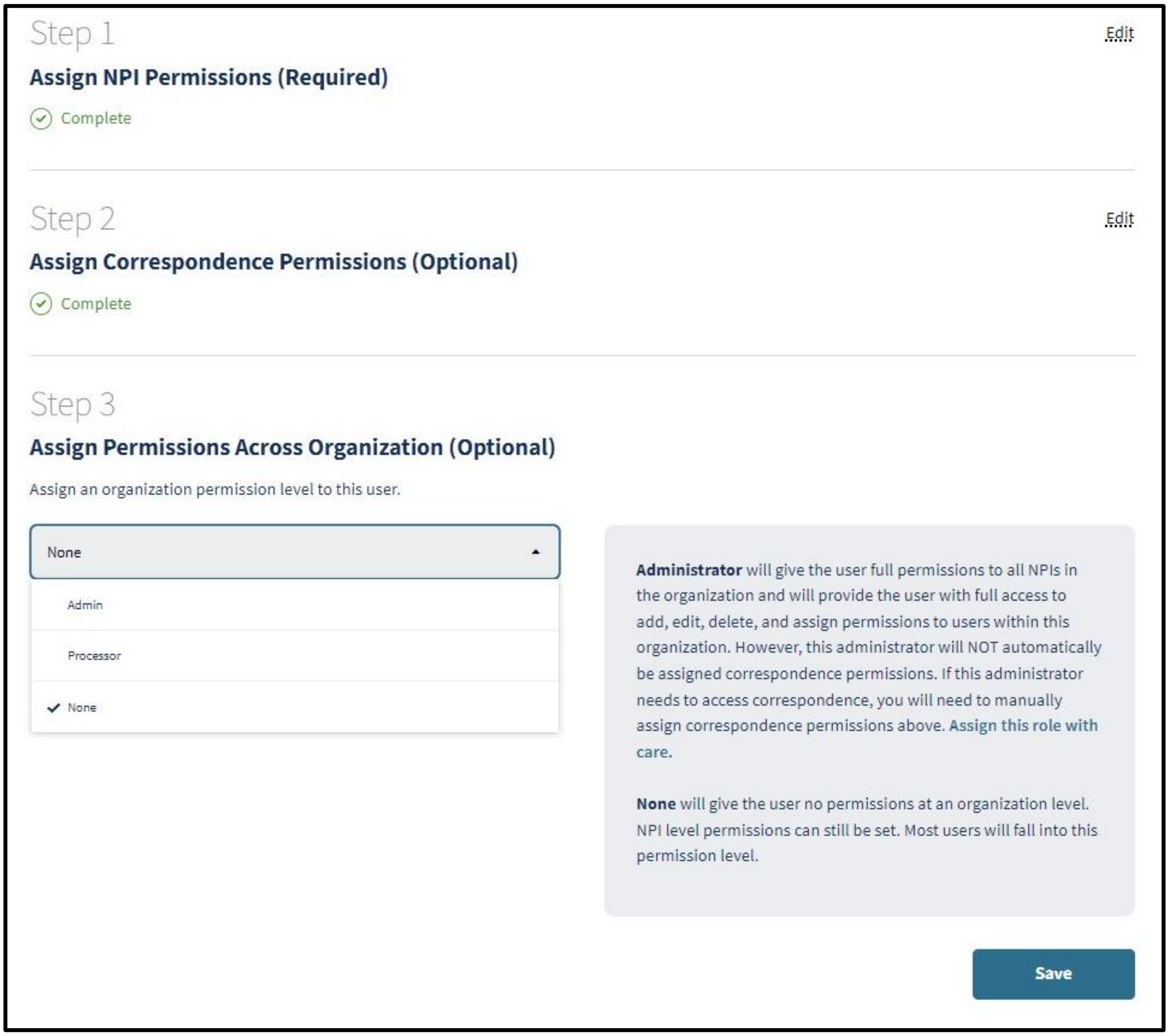


Figure 1.26: Step 3 Assign Permissions Across Organization.

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.

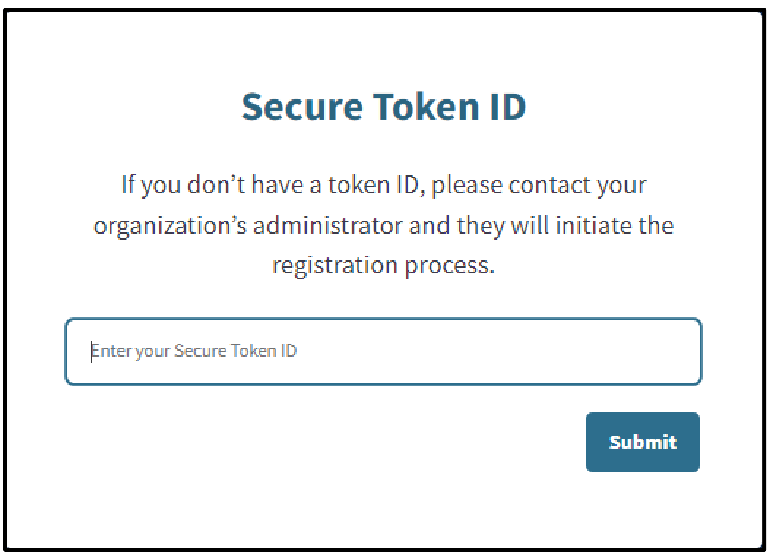


Figure 1.28: Secure Token ID.

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

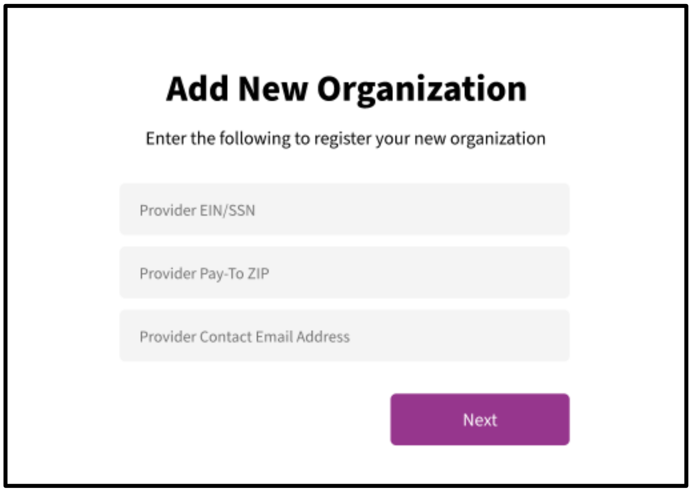


Figure 1.29: Add New Organization.

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

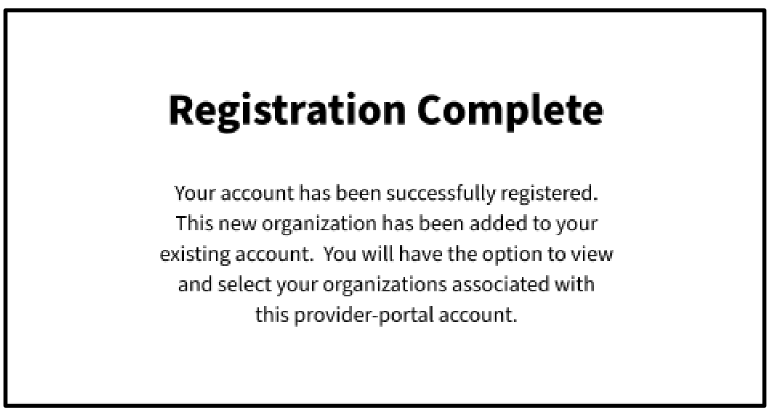


Figure 1.30: Registration Complete.

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.

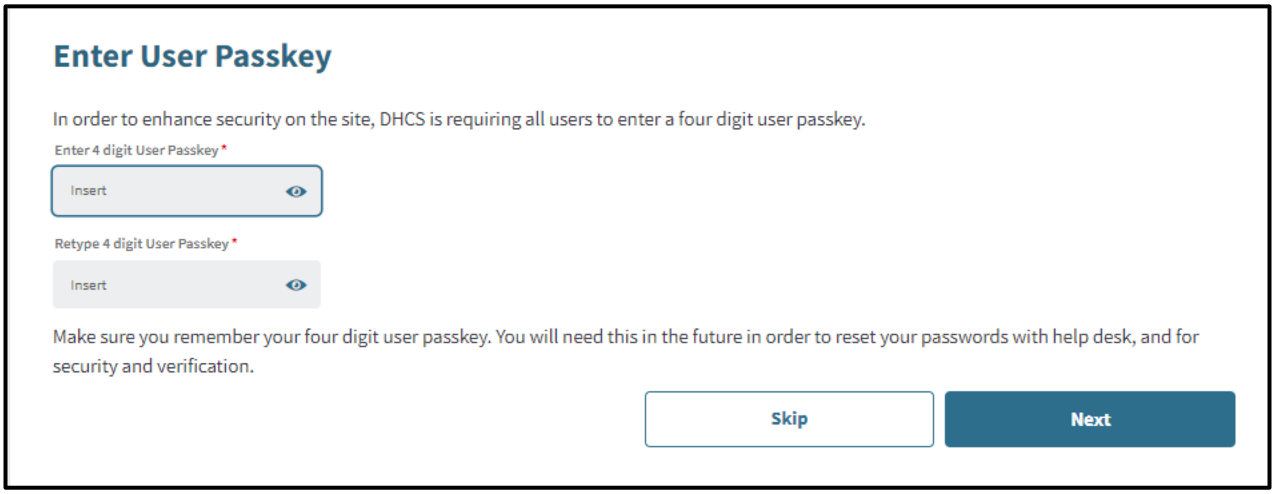


Figure 1.31: Enter User Passkey.

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

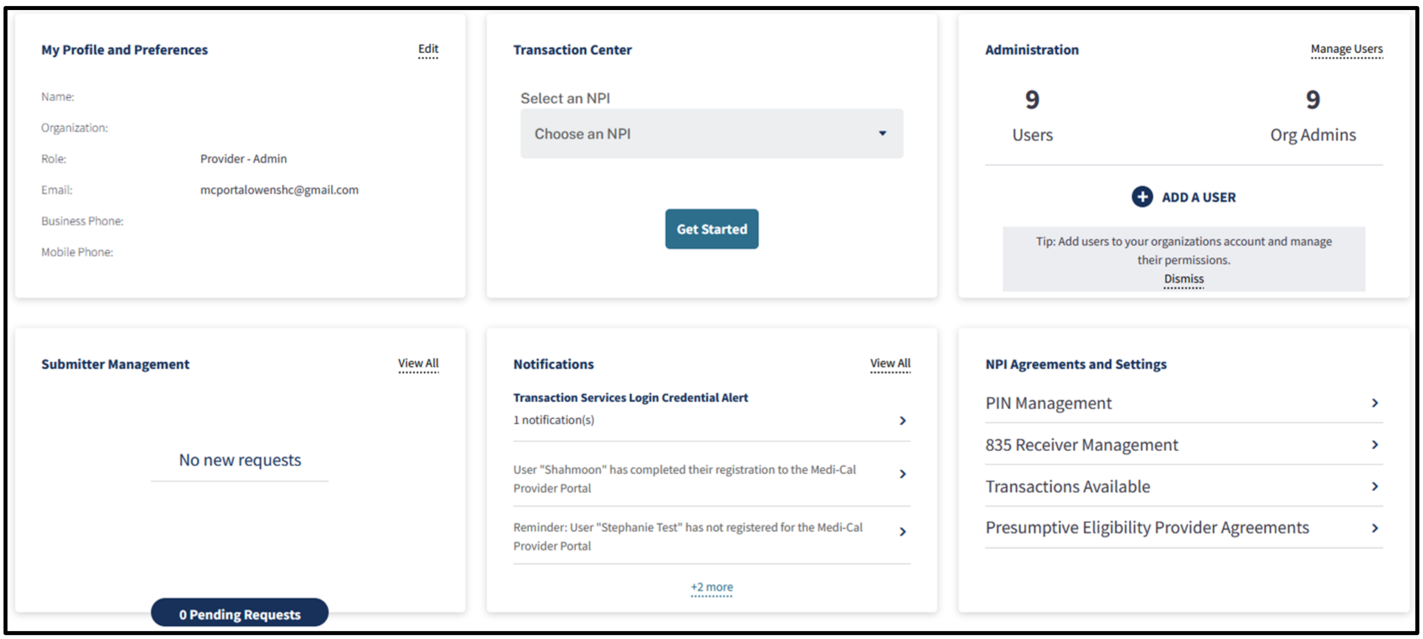


Figure 1.32: Provider Admin Dashboard.

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.

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.

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.

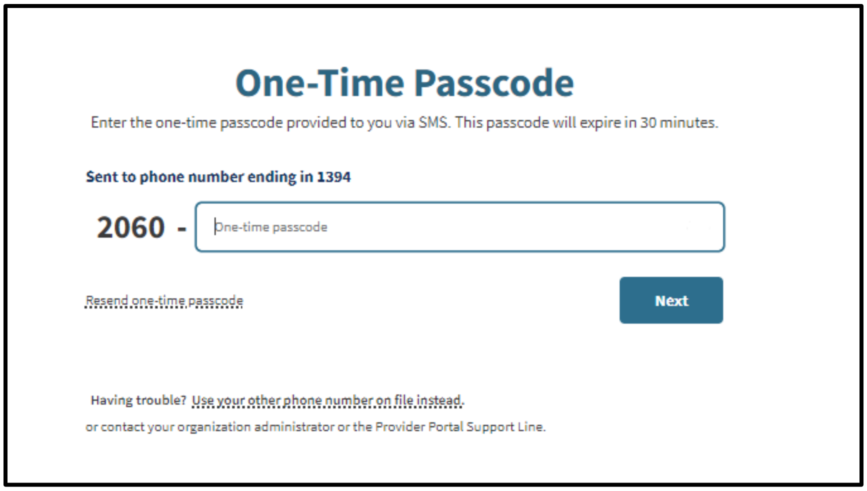


Figure 1.33: One-Time Passcode.

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.

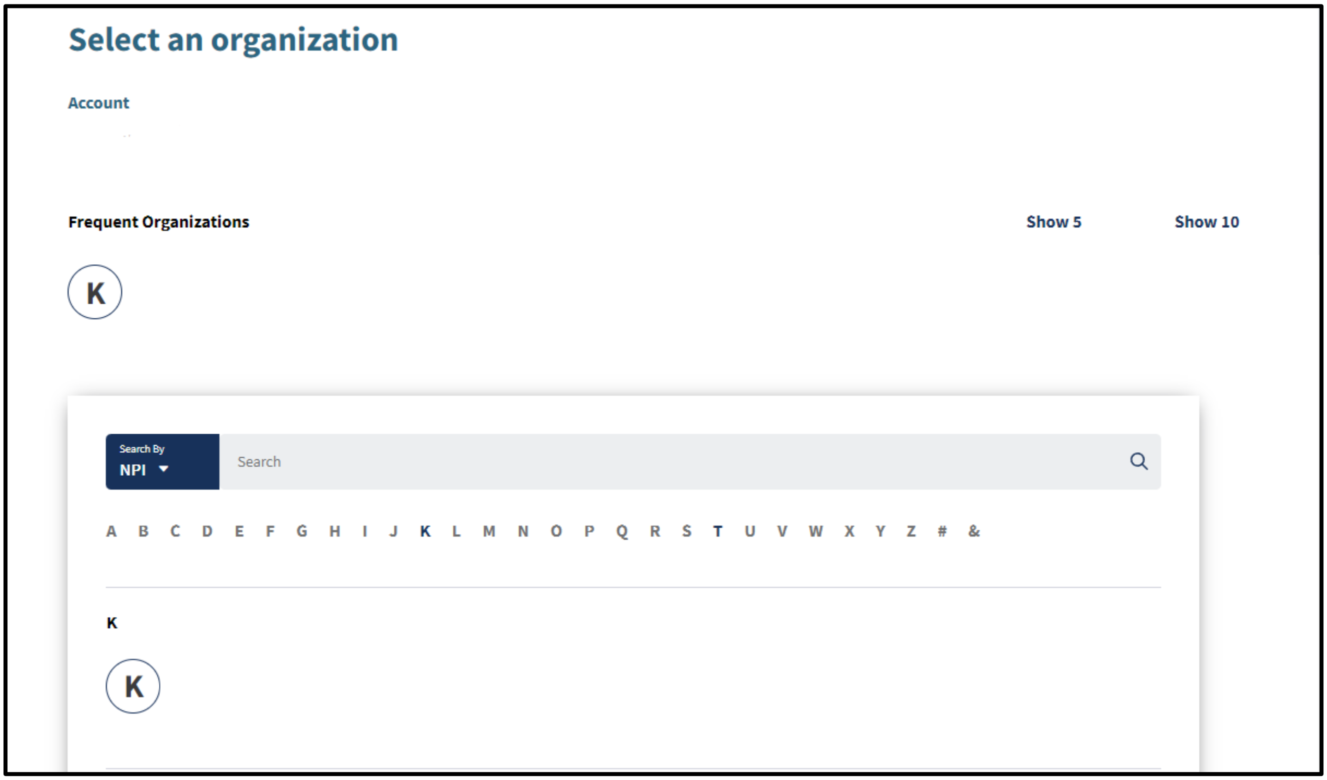


Figure 1.34: Select an Organization.

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.

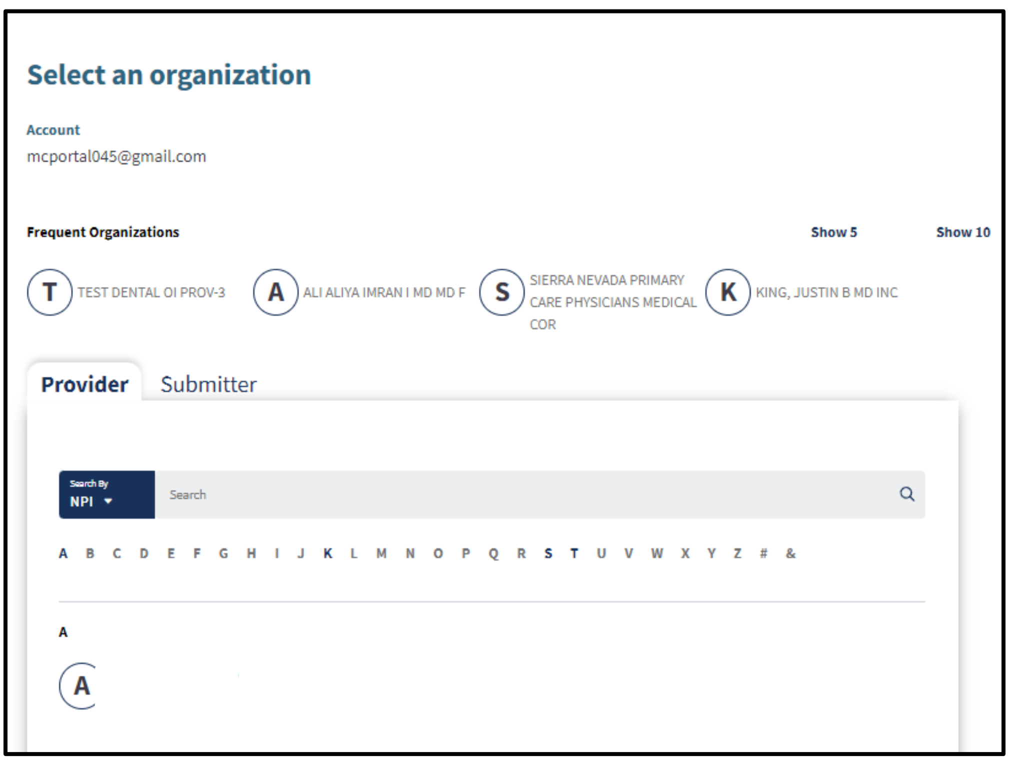


Figure 1.36: Select an Organization.

Change a Password

Users may change their own passwords:

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

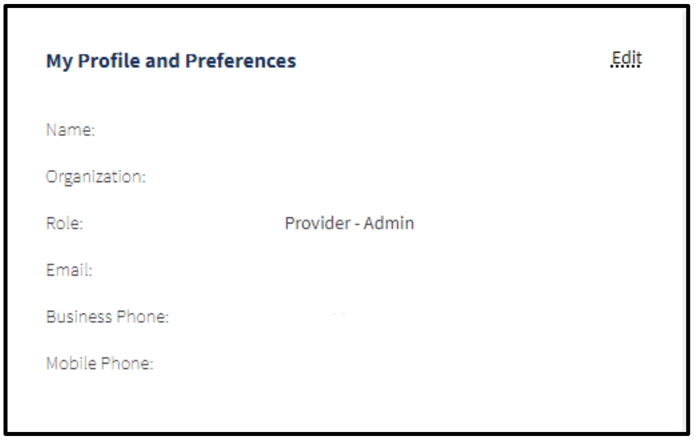


Figure 1.37: My Profile and Preferences.

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

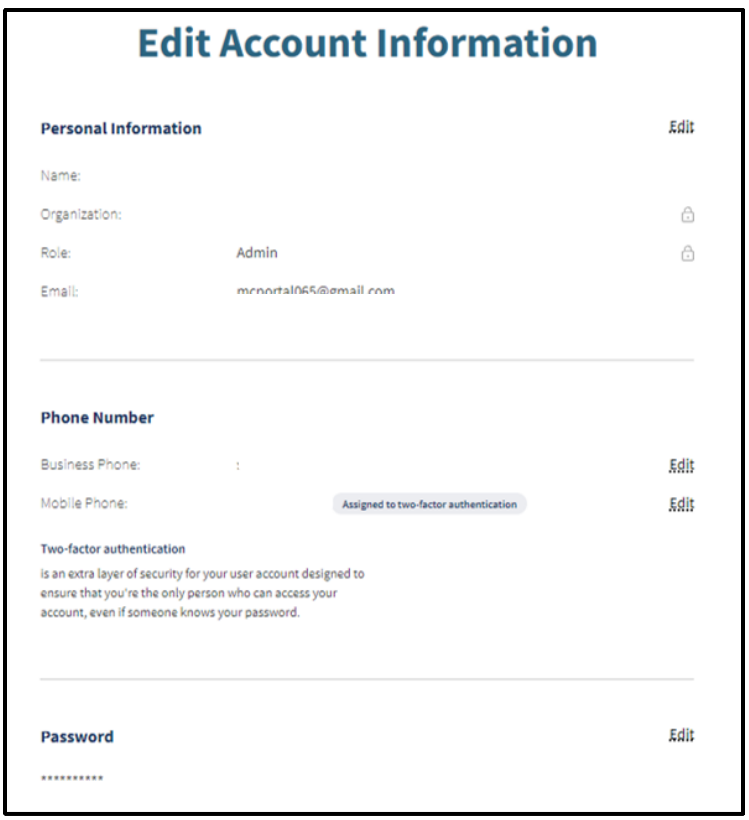


Figure 1.38: Edit Account Information.

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.**

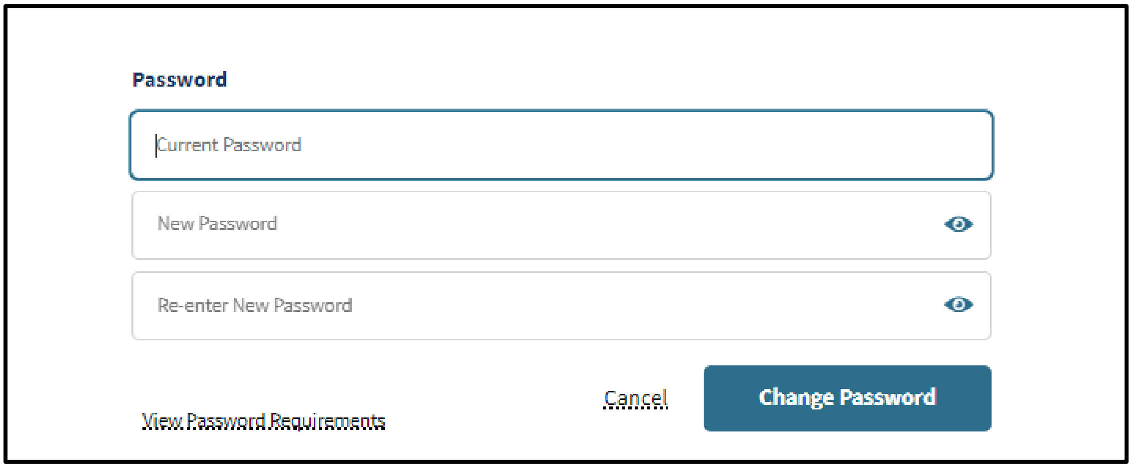


Figure 1.39: Change Password.

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.**

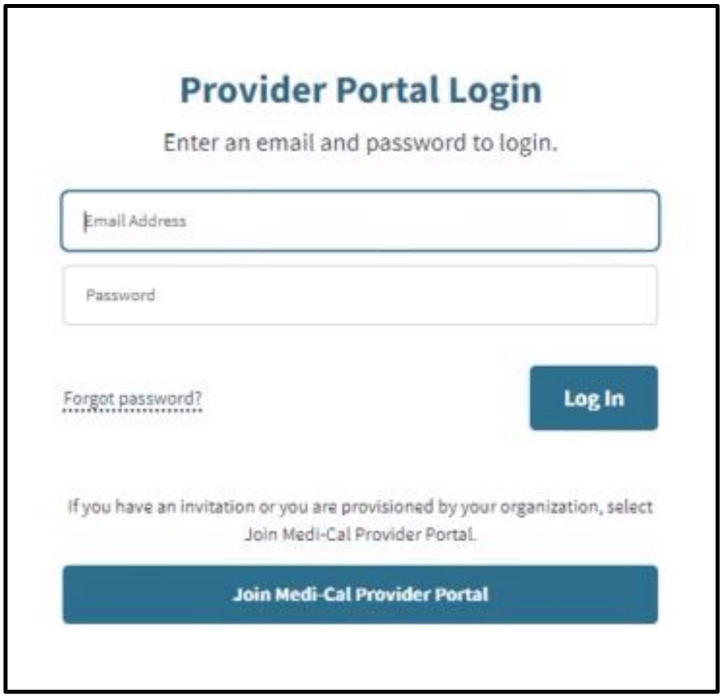


Figure 1.40: Medi-Cal Provider Portal Log In.

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

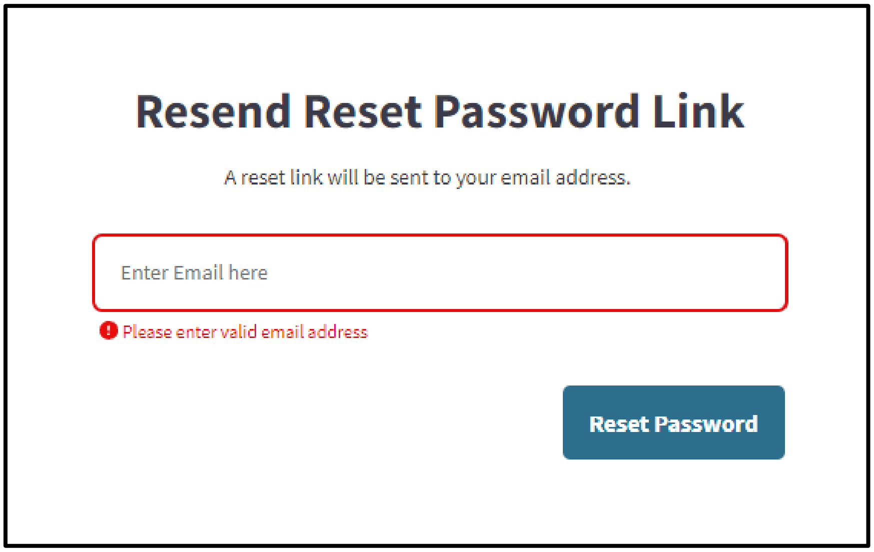


Figure 1.41: Resend Reset Password Link.

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

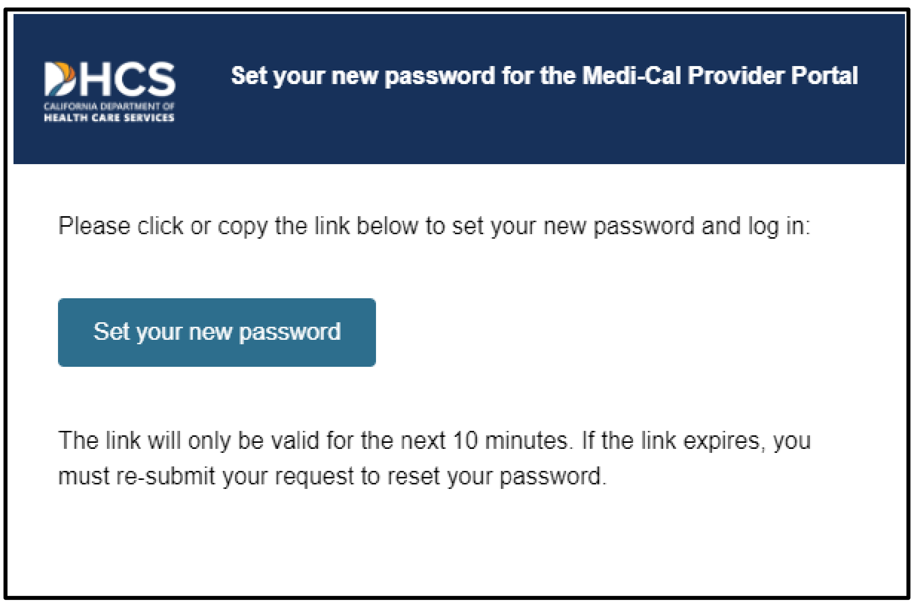


Figure 1.42: Set new password email notification.

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**.

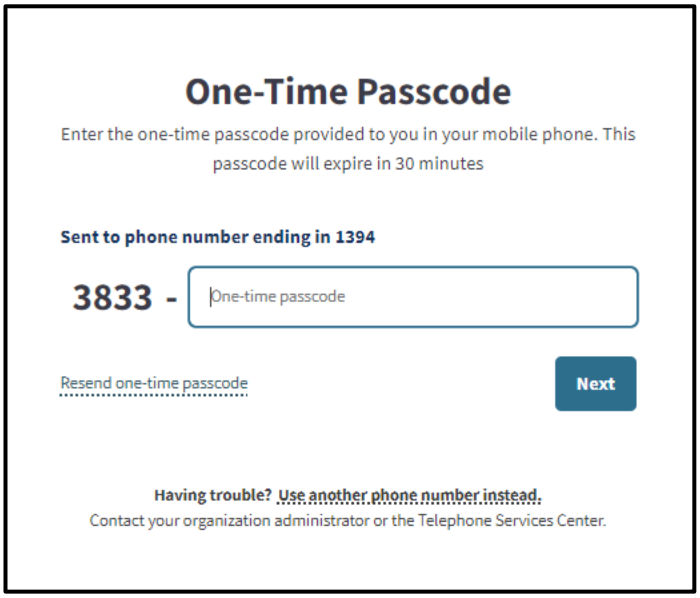


Figure 1.43: Enter One-Time Passcode.

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.

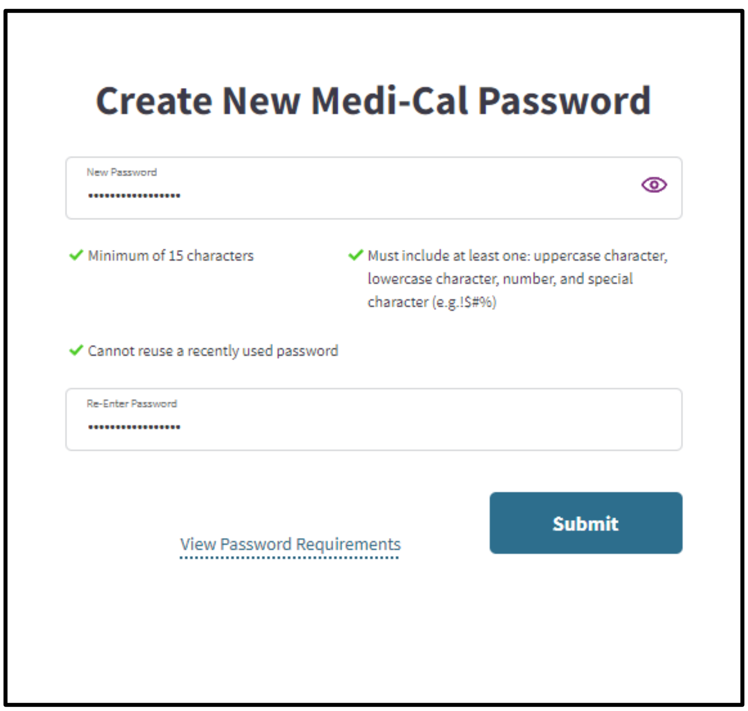


Figure 1.44: Create New Medi-Cal Password.

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.

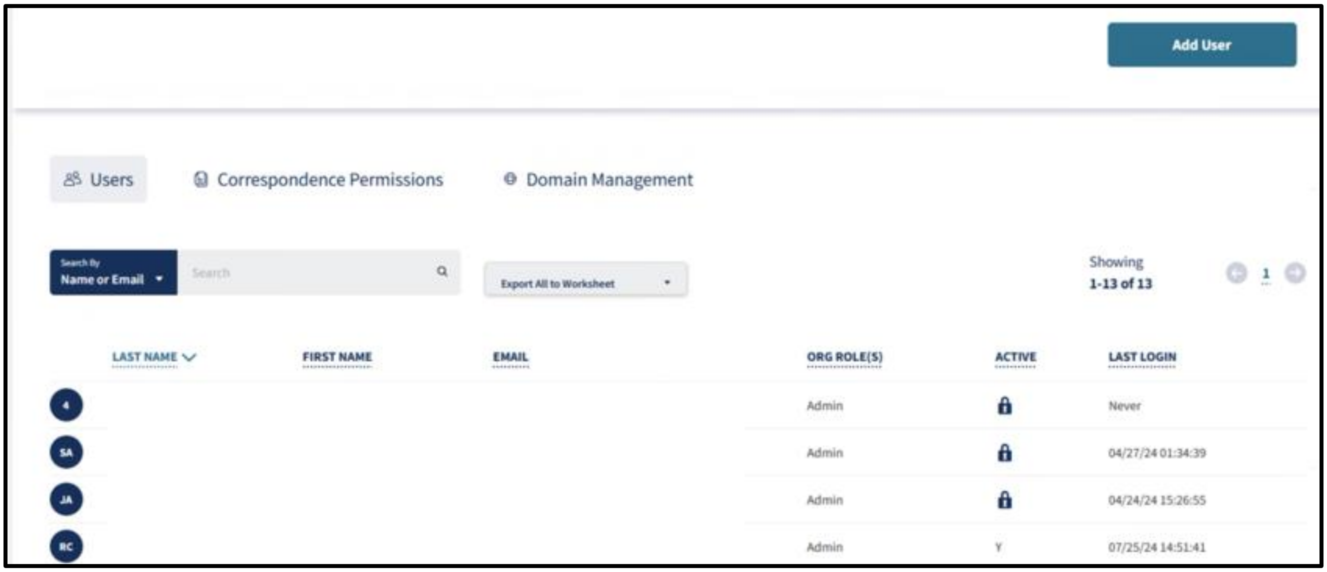


Figure 1.45: User Management.

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.

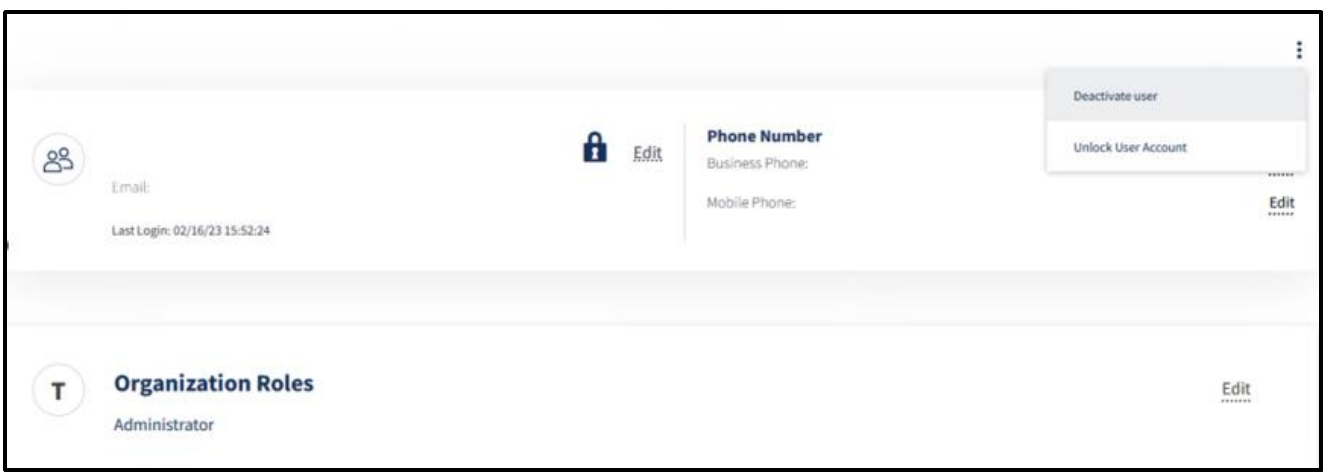


Figure 1.46: Unlock User Account.

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

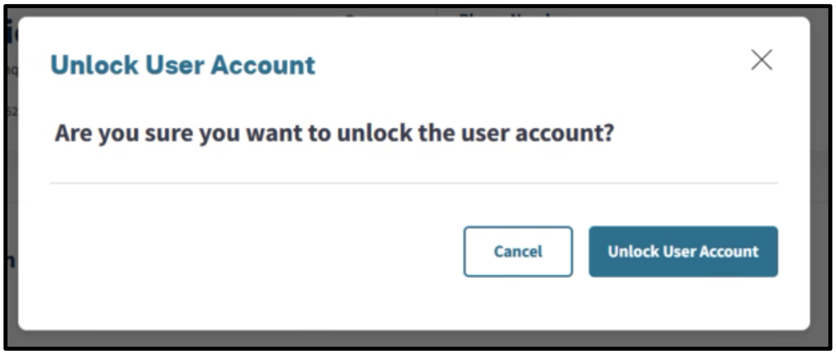


Figure 1.47: Unlock User Account.

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.

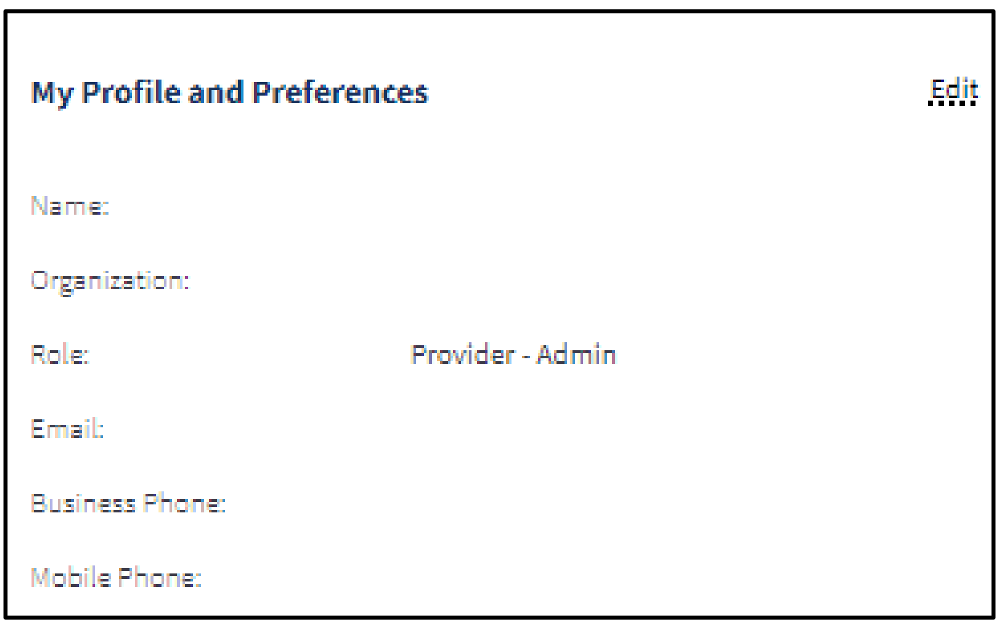


Figure 1.48: My Profile and Preferences.

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

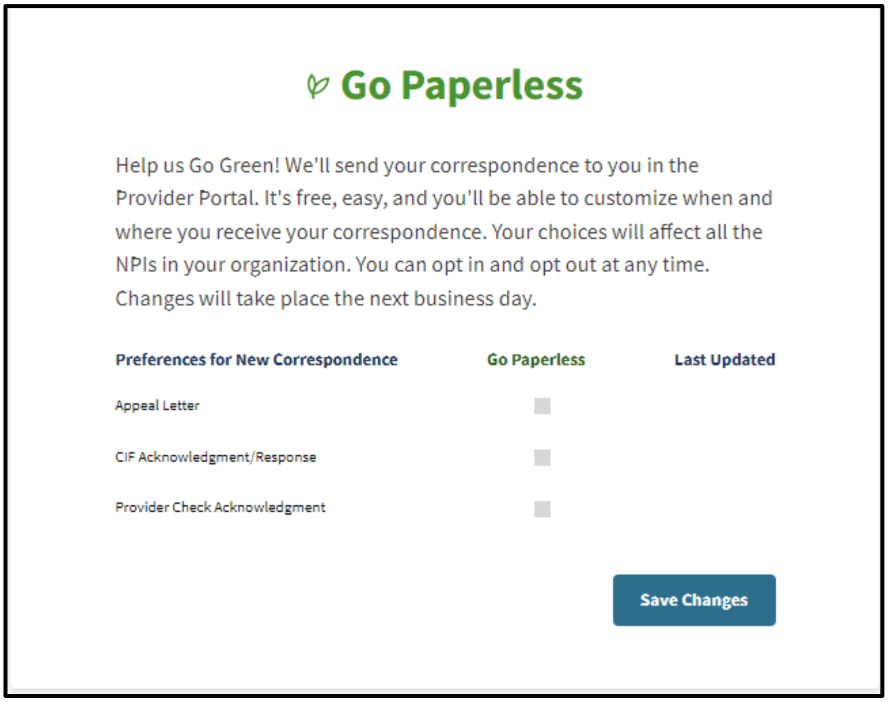


Figure 1.49: Go Paperless.

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

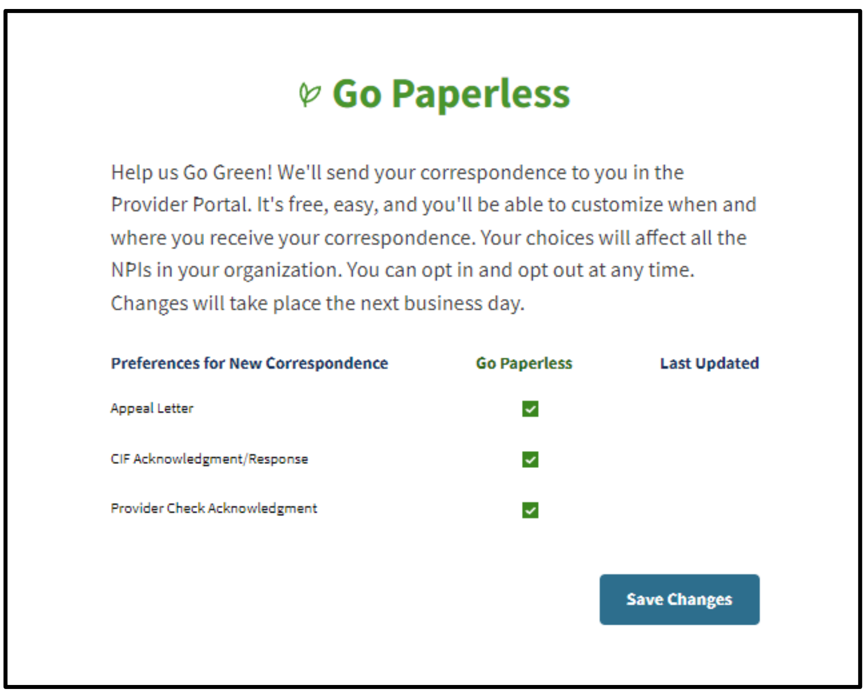


Figure 1.50: Go Paperless enrollment.

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

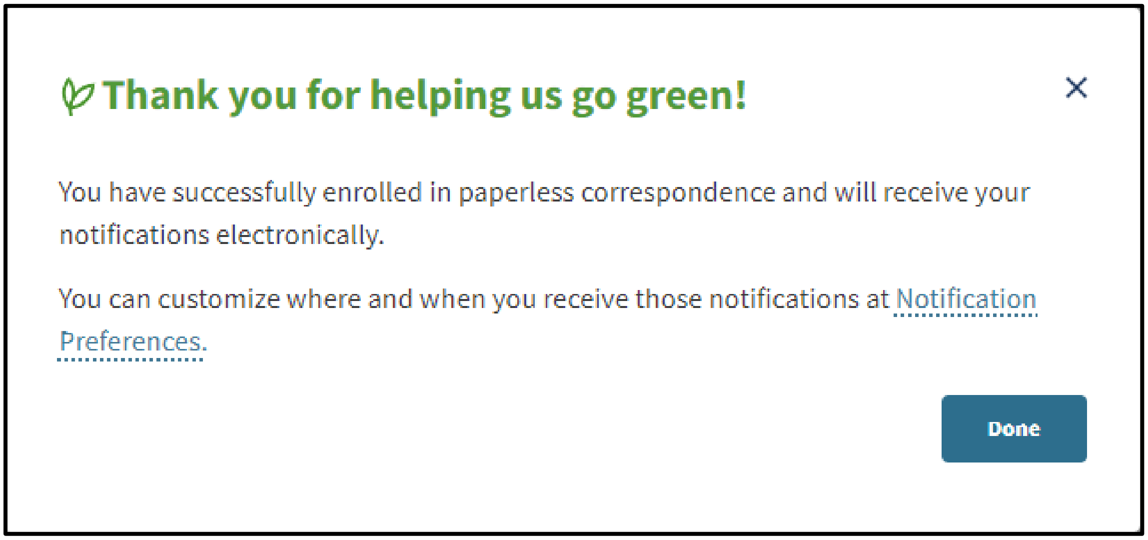


Figure 1.51: Go Paperless enrollment confirmation.

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**:

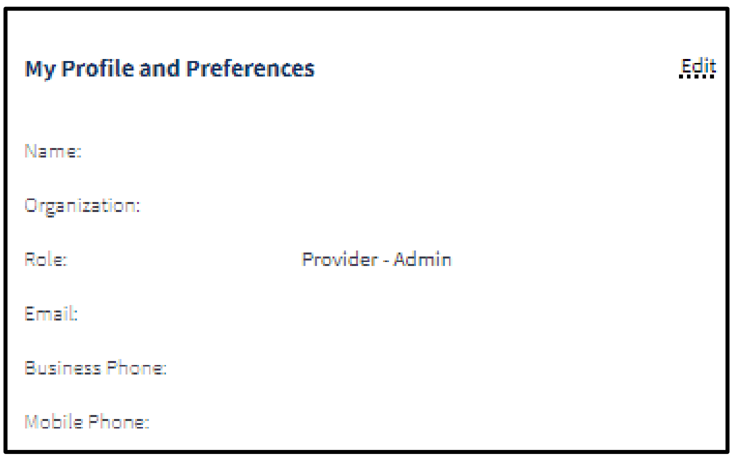


Figure 2.1: My Profile and Preferences.

Edit Personal Information

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

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

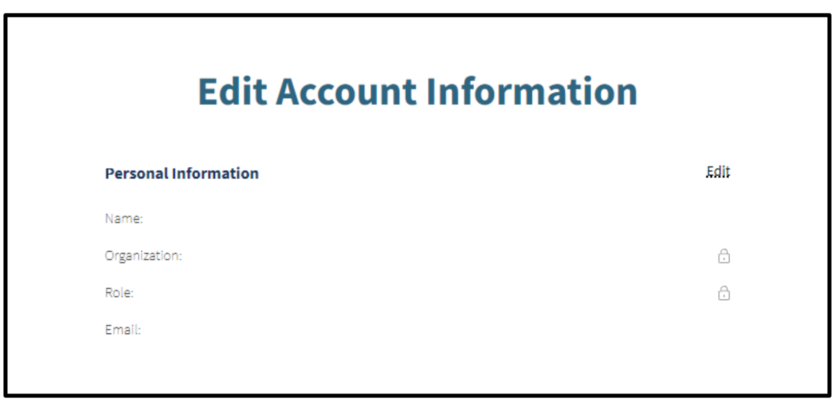


Figure 2.2: Edit Account Information.

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

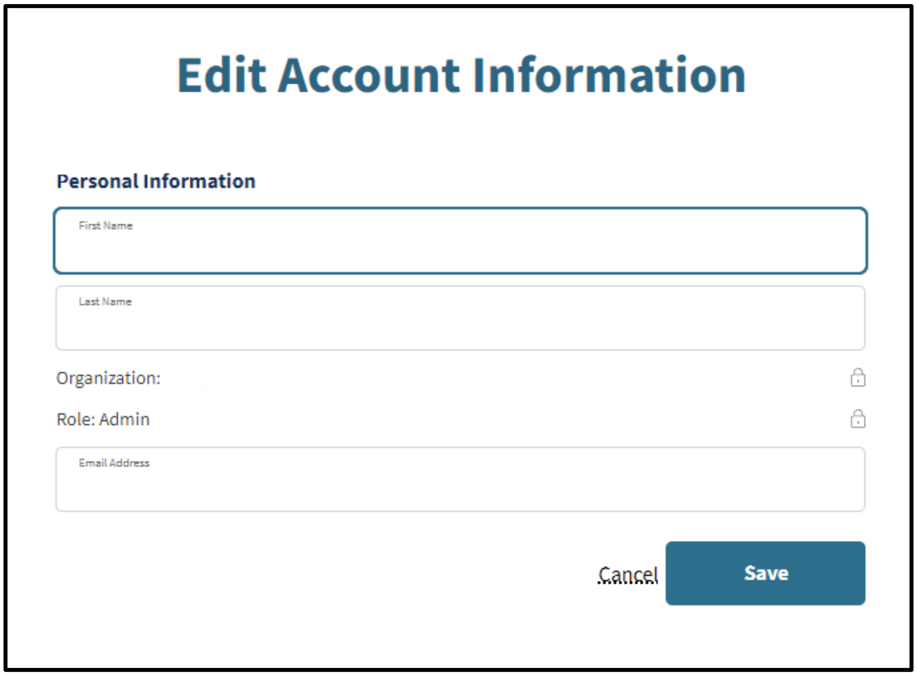


Figure 2.3: Edit Personal Information.

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.

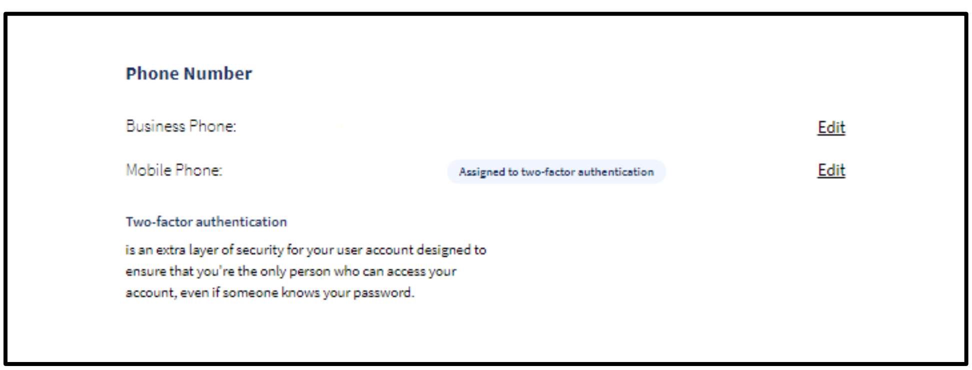


Figure 2.4: Phone Number.

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**.

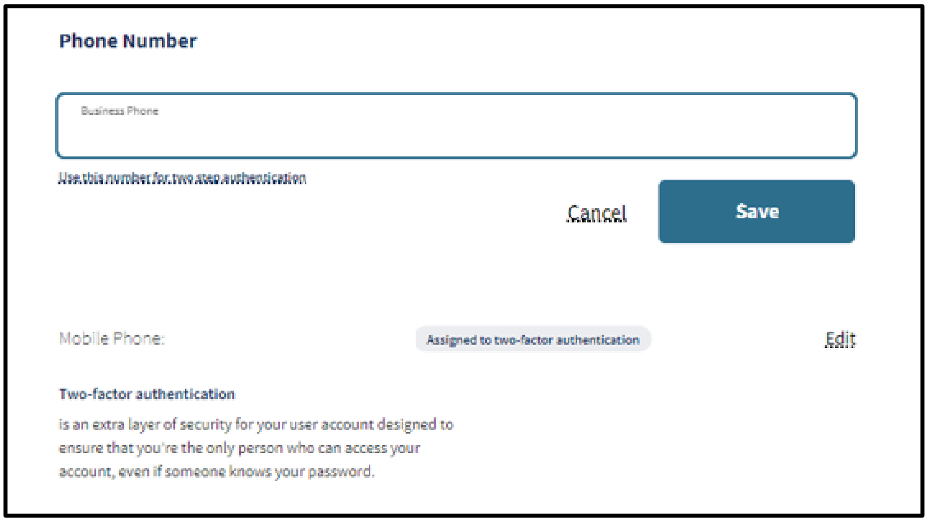


Figure 2.5: Edit Phone Number.

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

Edit Passkey

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

Figure 2.6: Edit Passkey.

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.

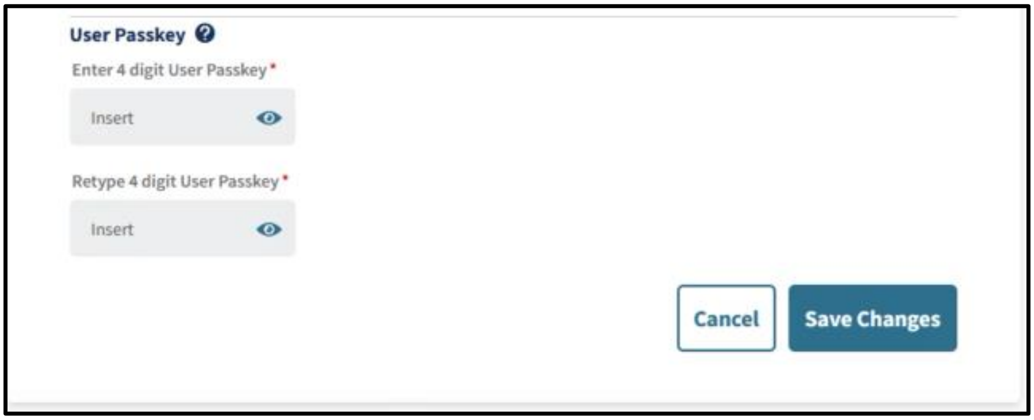


Figure 2.7: Edit Passkey.

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

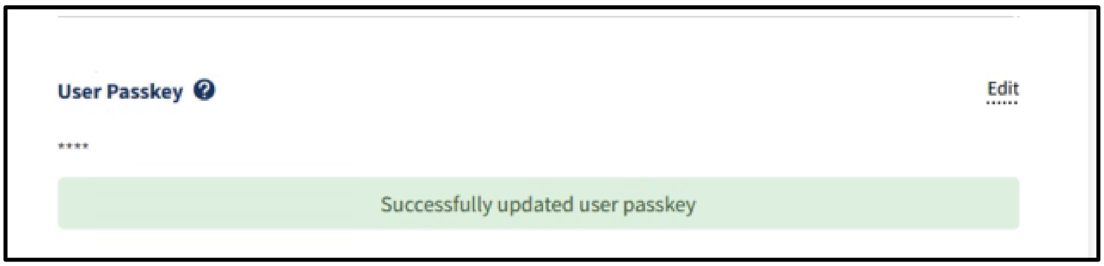


Figure 2.8: Successfully Updated User Passkey.

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**.

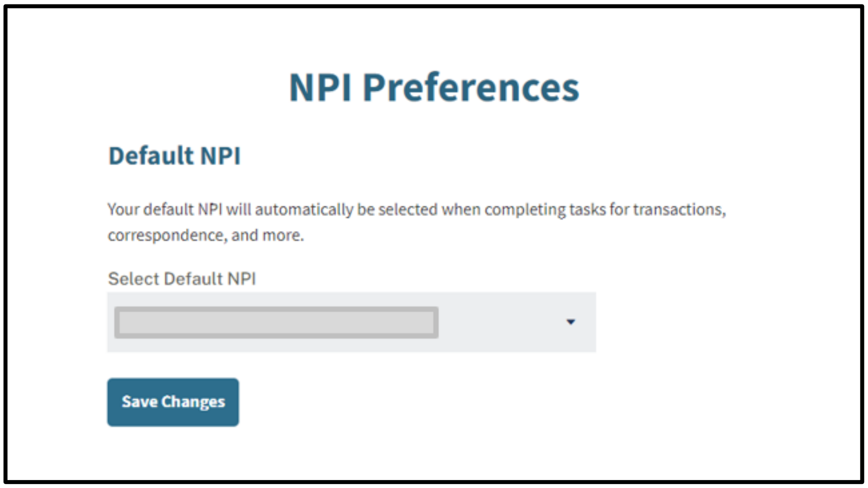


Figure 2.9: NPI Preferences.

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.

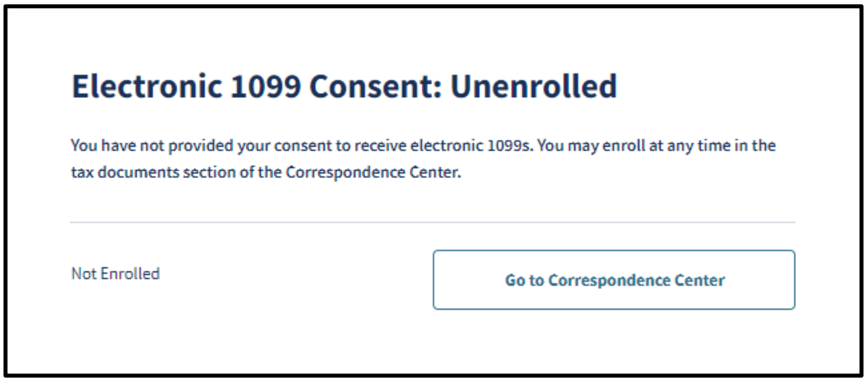


Figure 2.11: Electronic 1099 Consent.

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.

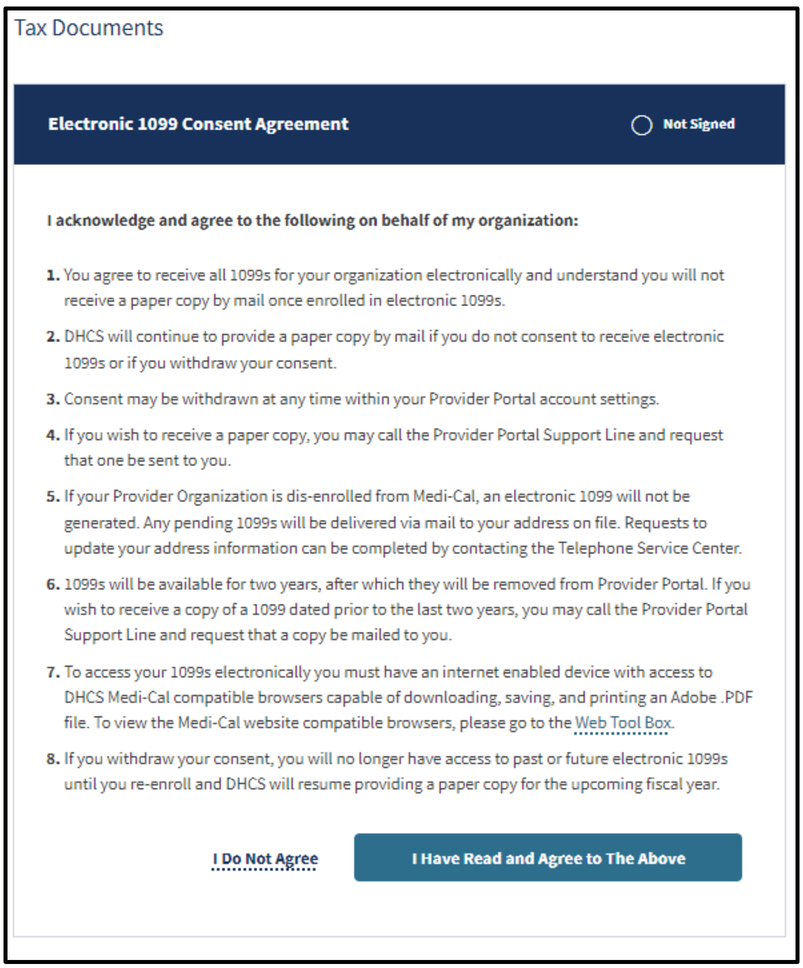


Figure 2.12: Electronic 1099 Consent Agreement.

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.

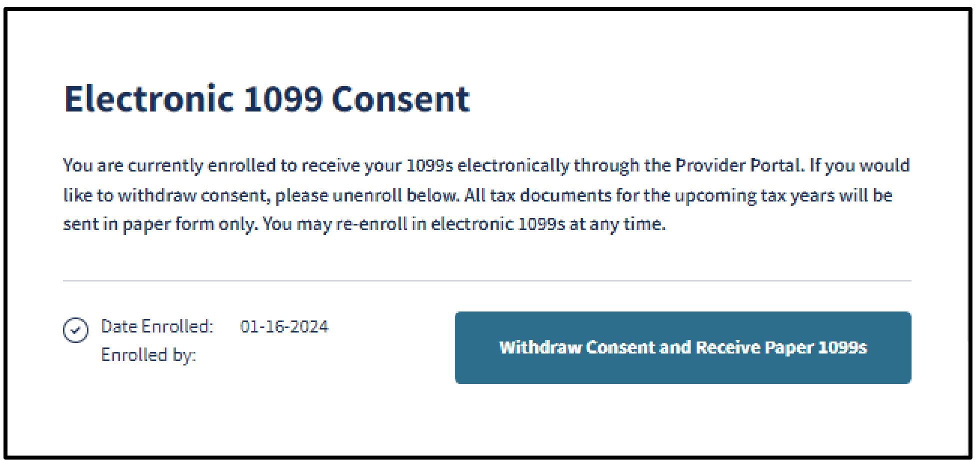


Figure 2.14: Electronic 1099 Consent Withdrawal.

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

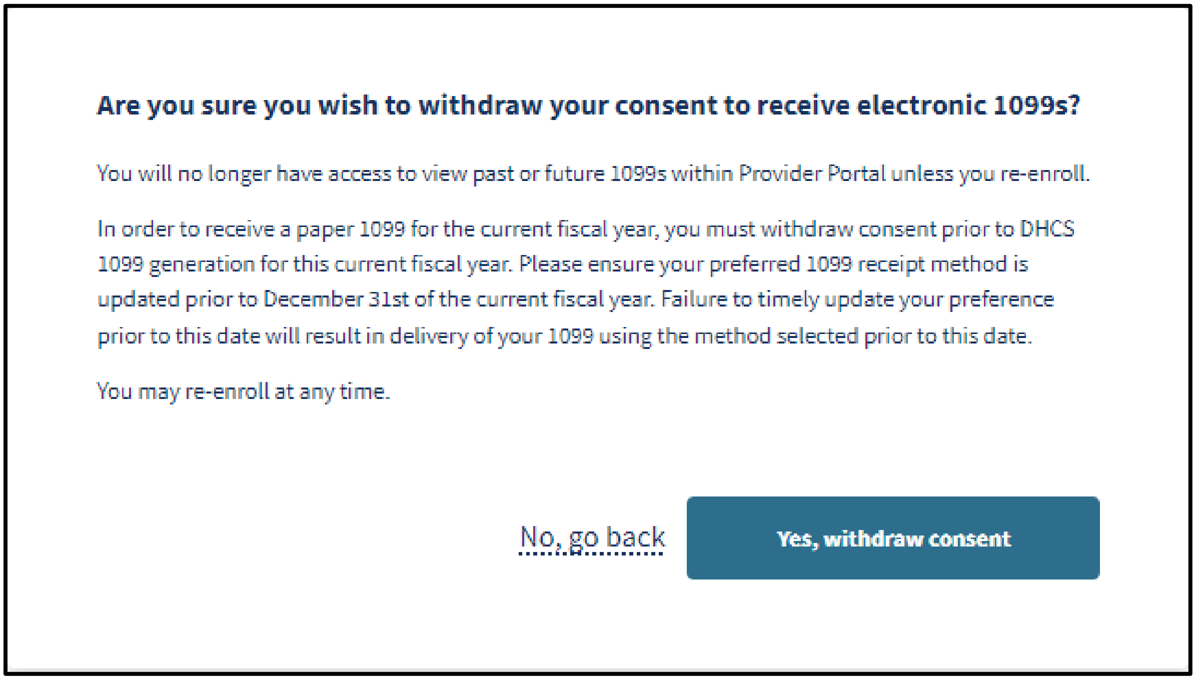


Figure 2.15: Withdraw consent to receive electronic 1099s.

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.

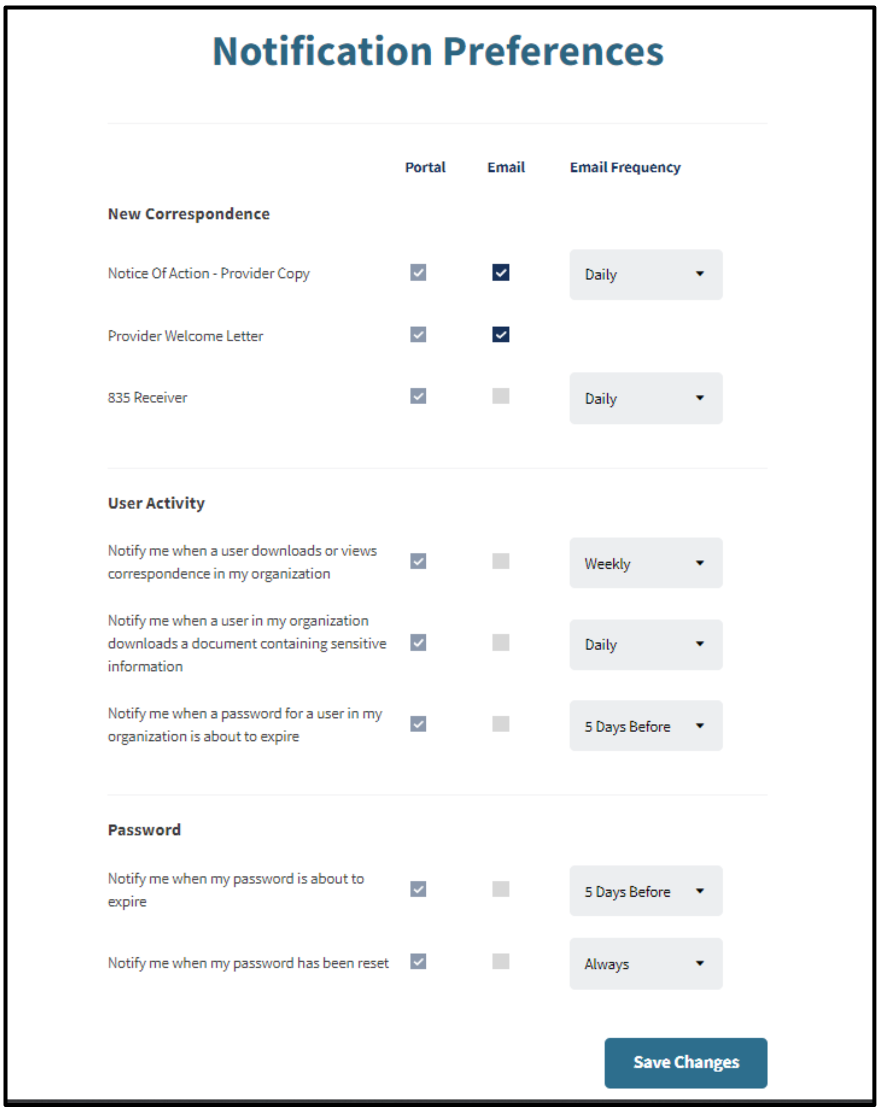


Figure 2.16: Edit Notification Preferences.

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

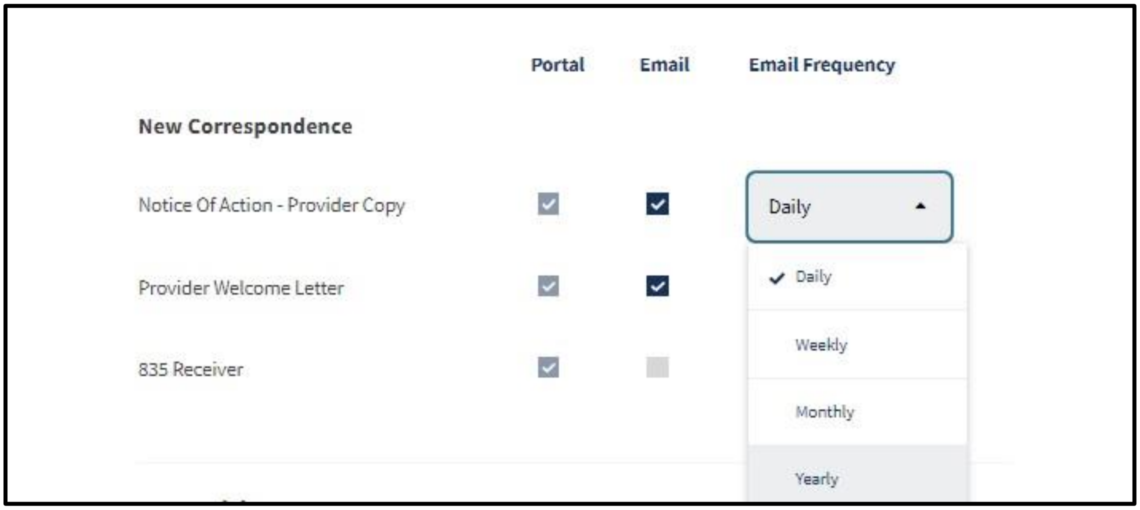


Figure 2.17: Edit Notification Frequency.

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

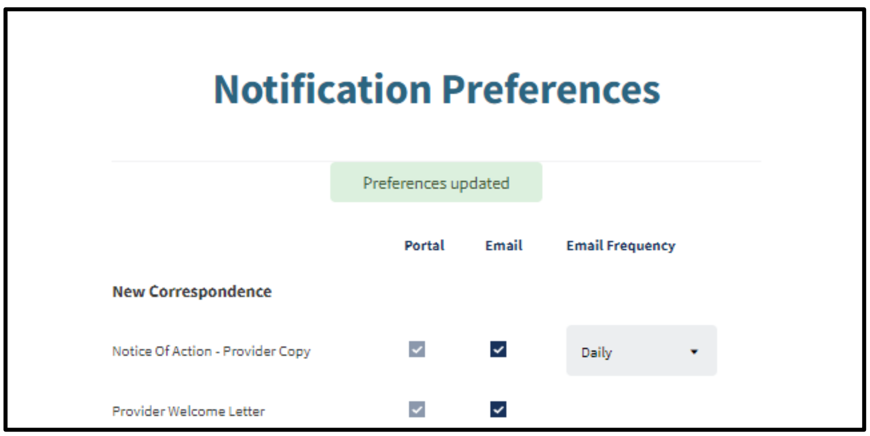


Figure 2.18: Notification Preference successfully updated.

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**.

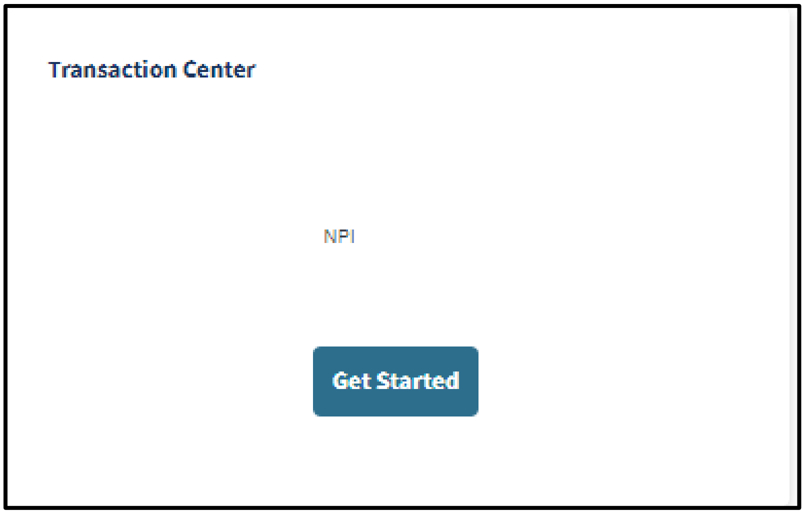


Figure 2.19: Transaction Center tile.

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.

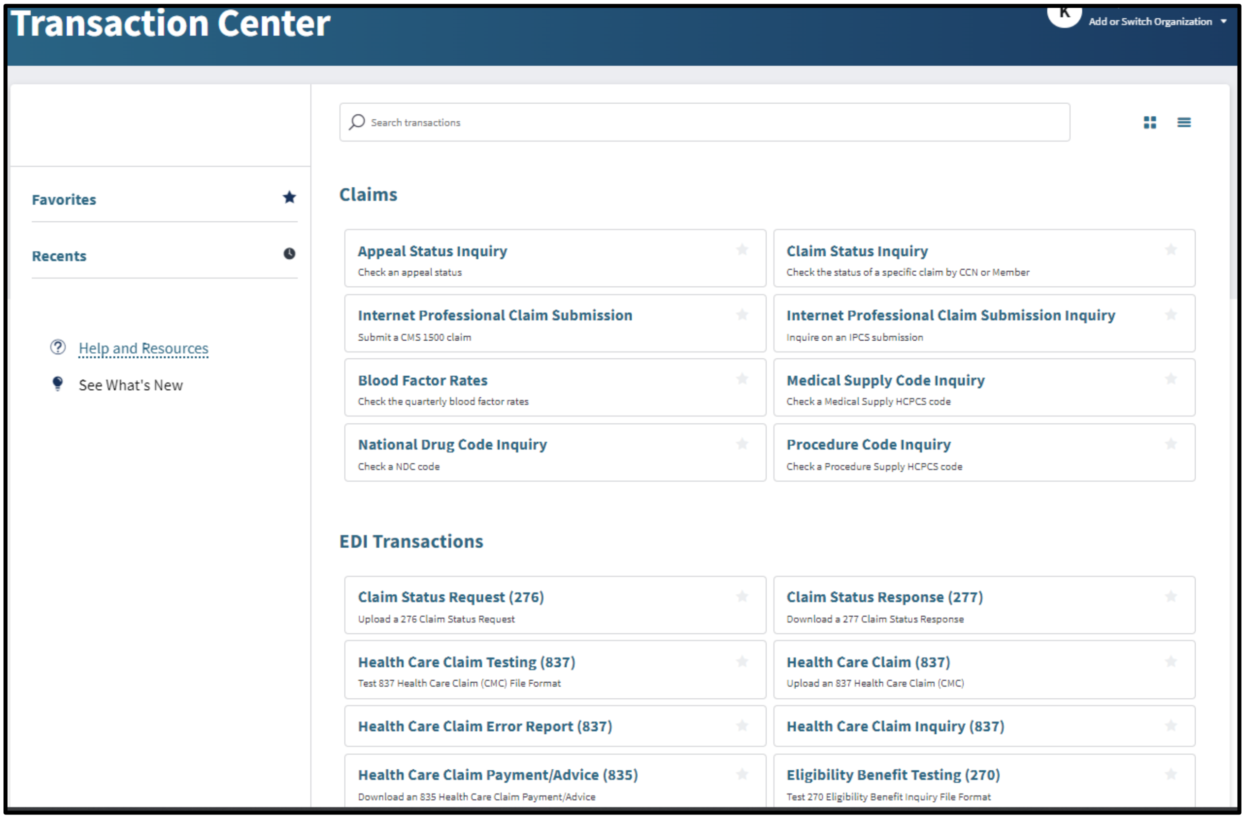


Figure 2.20: Transaction Center.

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.

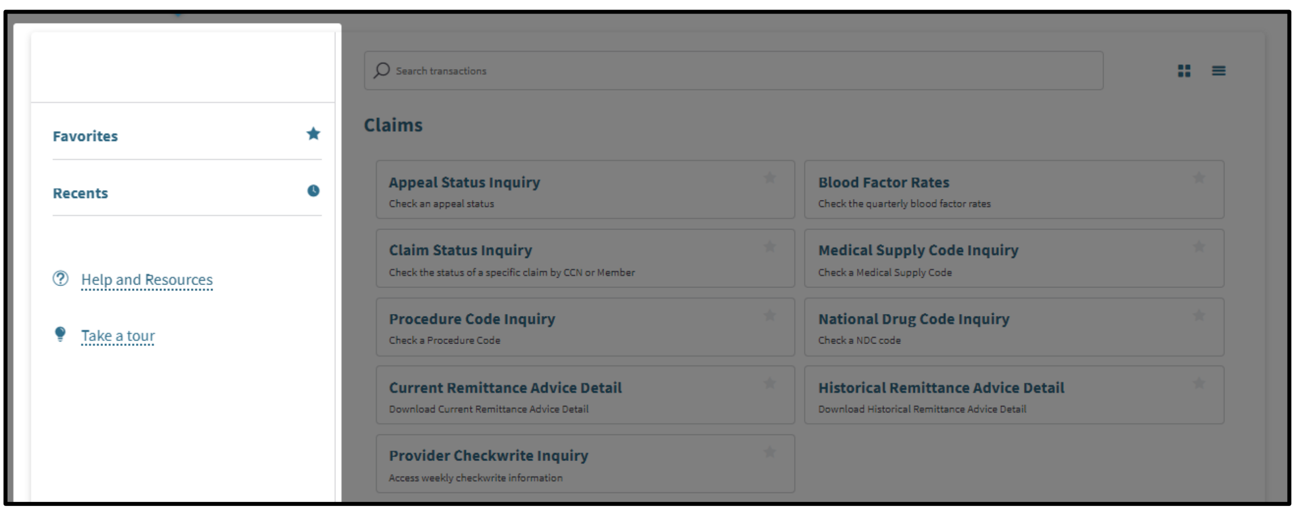


Figure 2.21: Side Panel Featuring Favorites and Recents.

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.

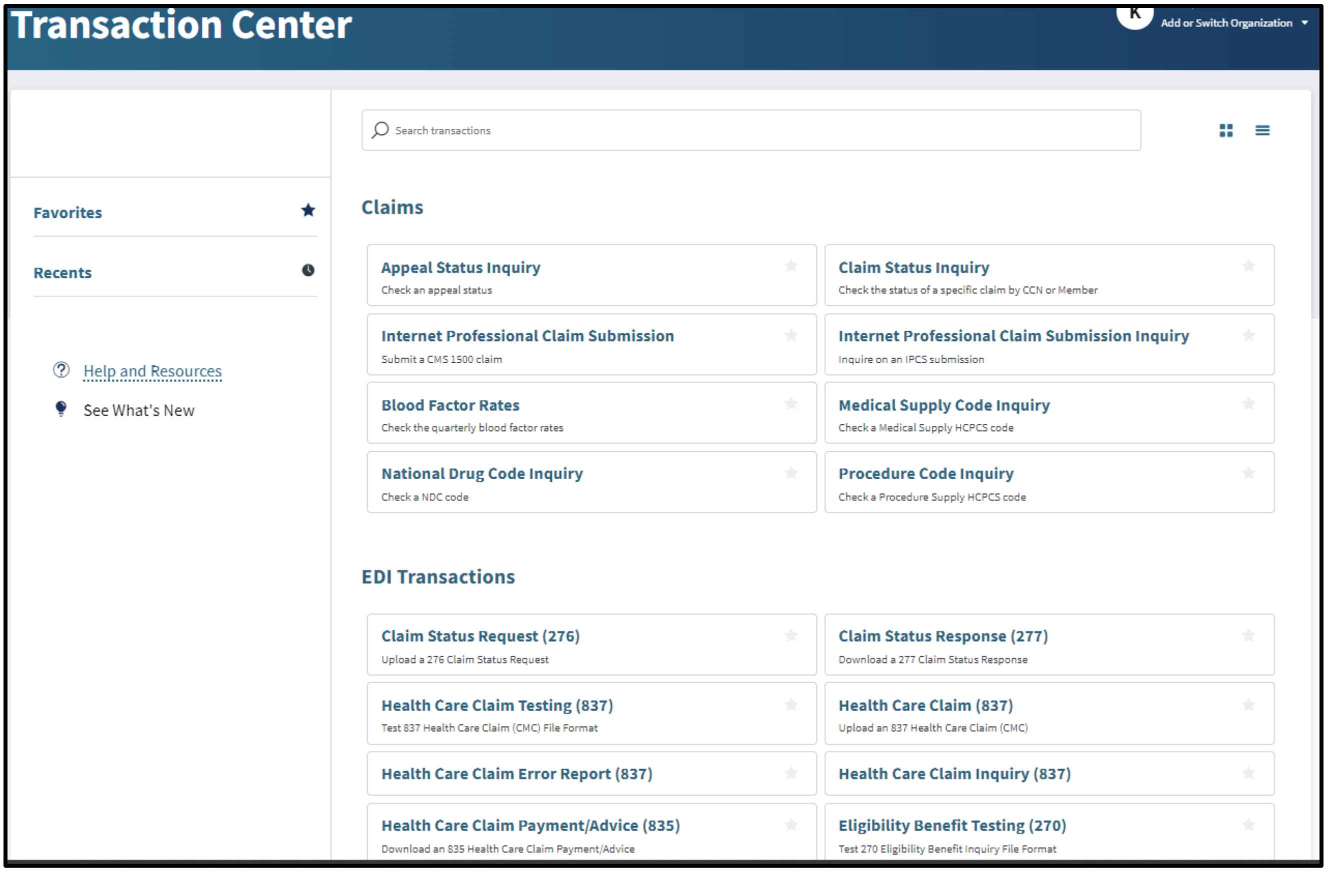


Figure 2.22: Transaction Center.

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

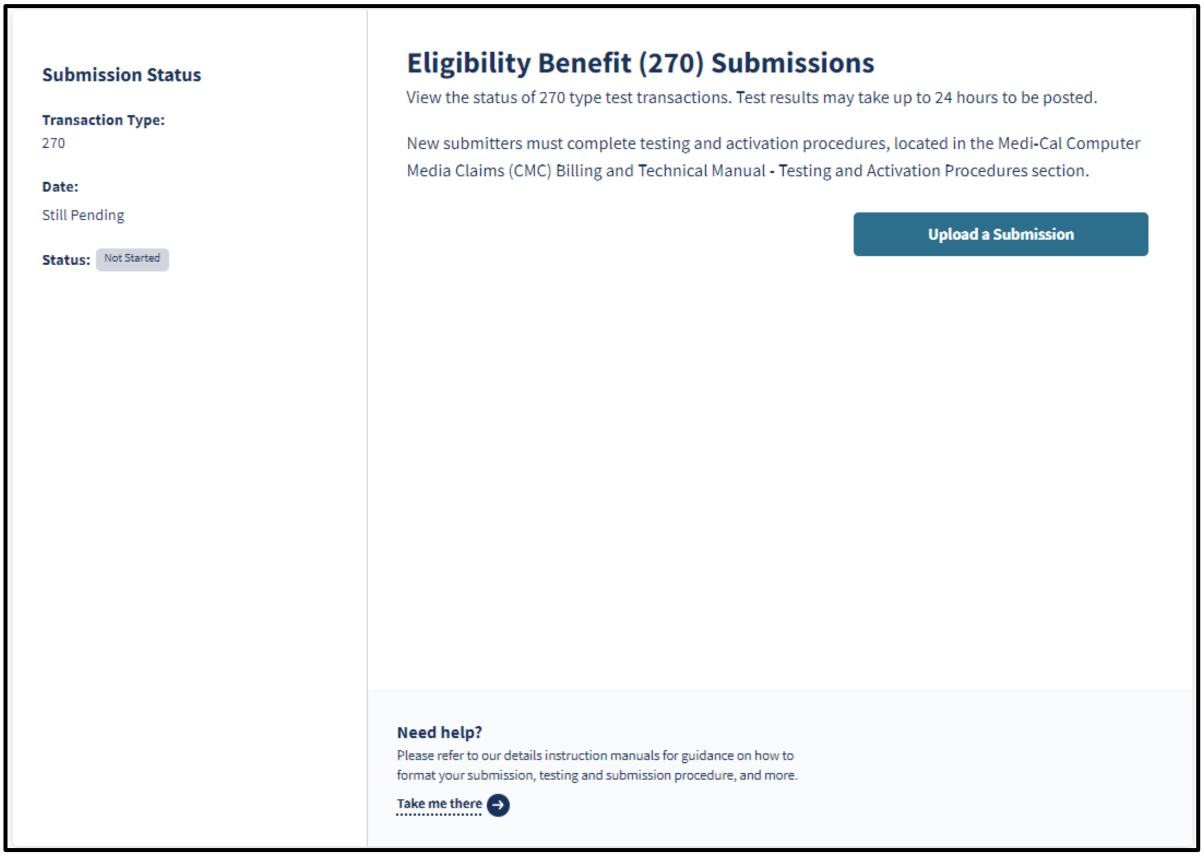


Figure 2.23: Eligibility Benefit (270) Submissions.

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.

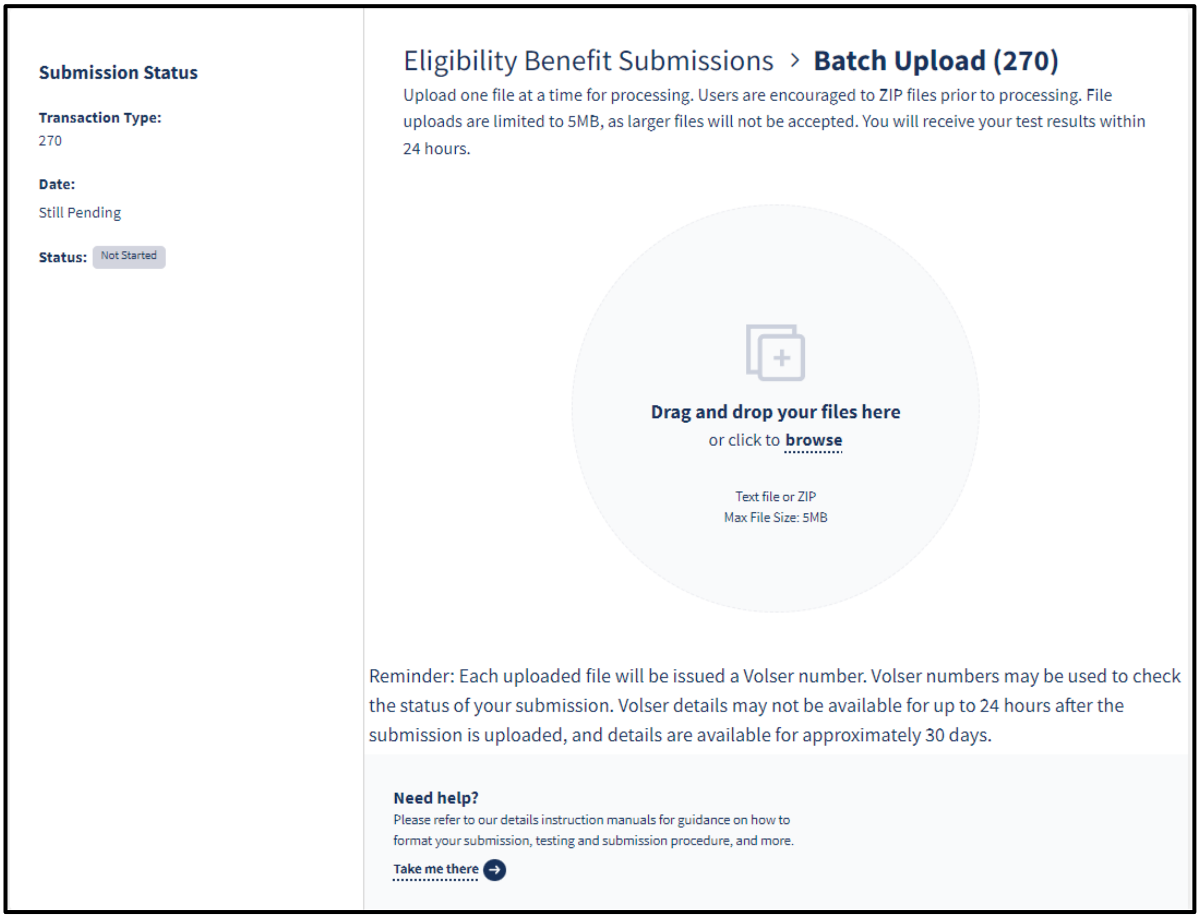


Figure 2.24: Eligibility Benefit (270) upload.

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

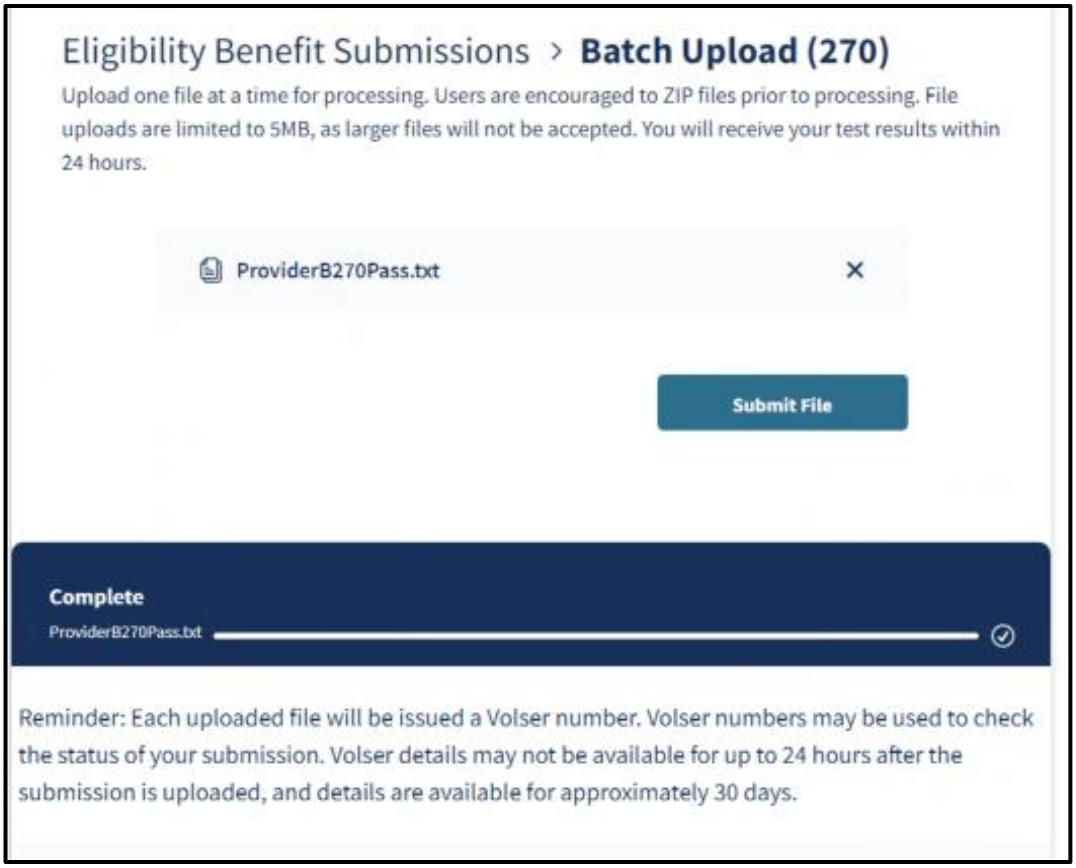


Figure 2.25: Eligibility Benefit (270) Submit File.

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

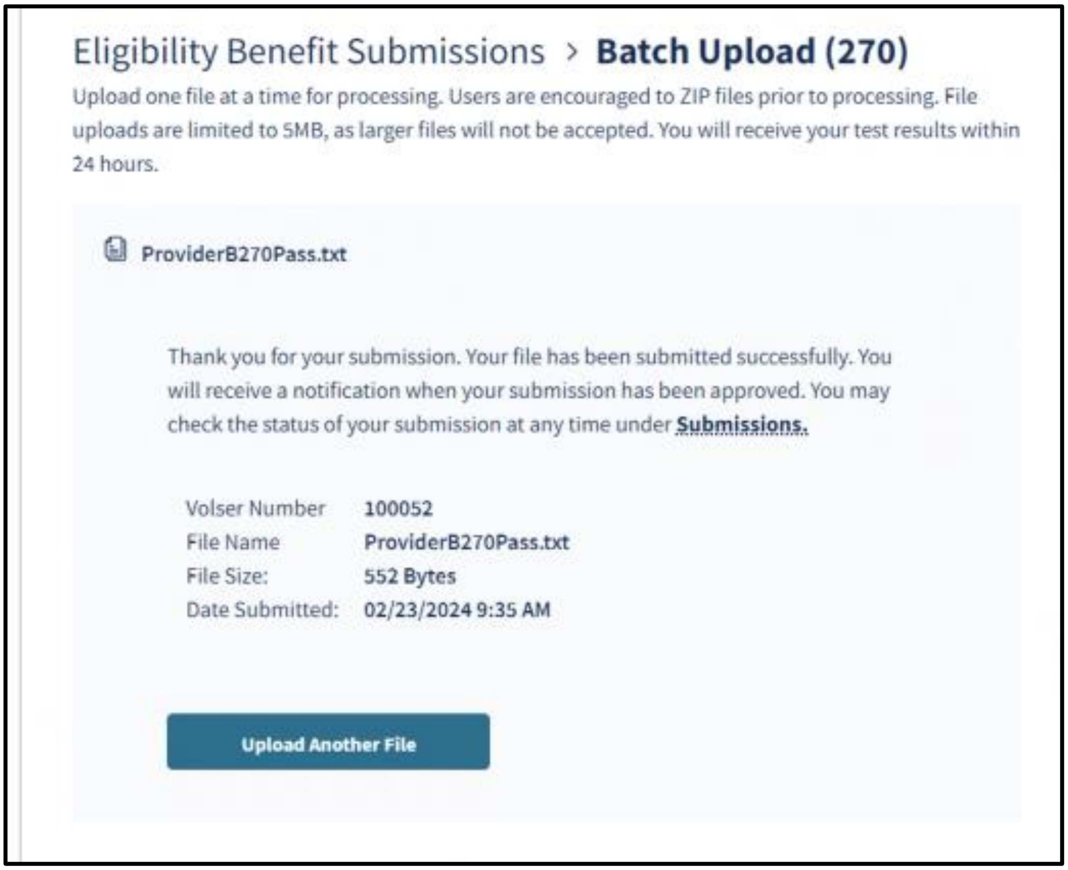


Figure 2.26: Eligibility Benefit (270) upload submission.

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

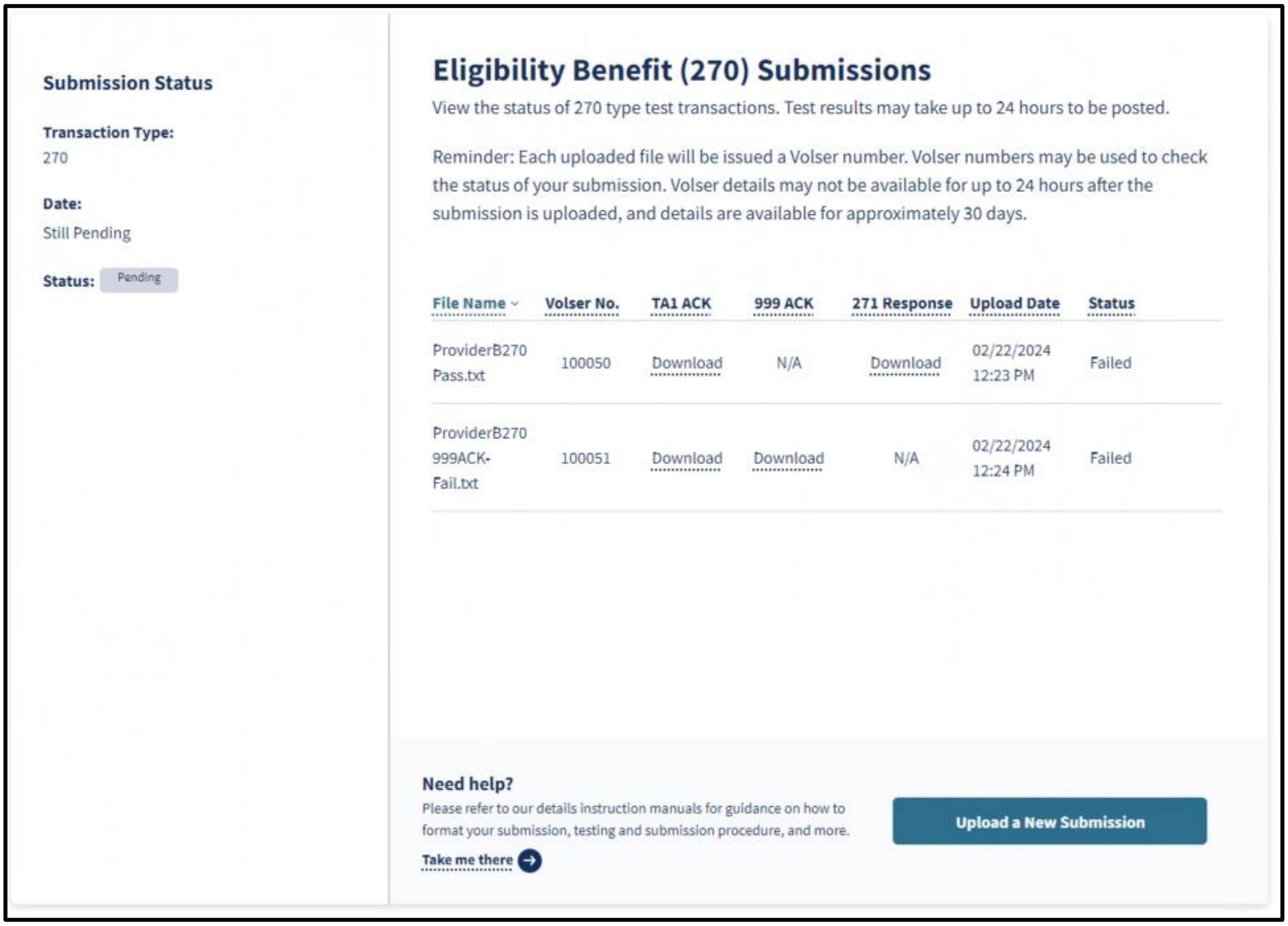


Figure 2.27: Eligibility Benefit (270) submissions list.

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.

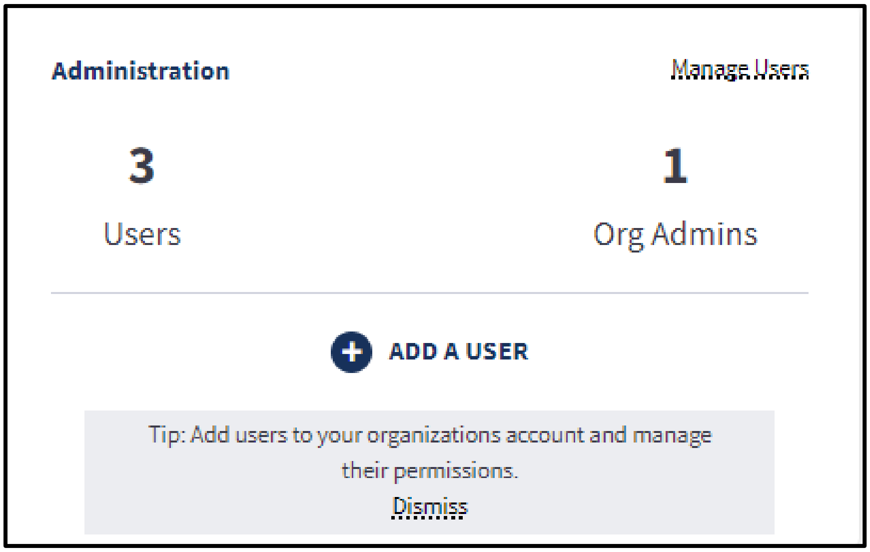


Figure 2.28: Administration Tile.

Updating User Information/Permissions

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

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

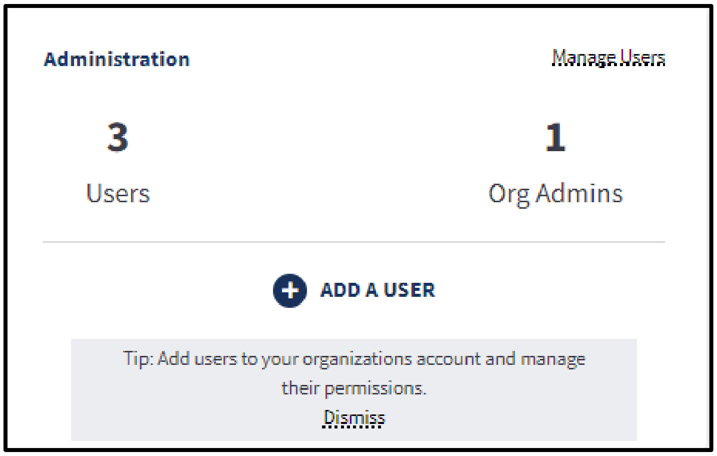


Figure 2.29: Administration Tile.

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

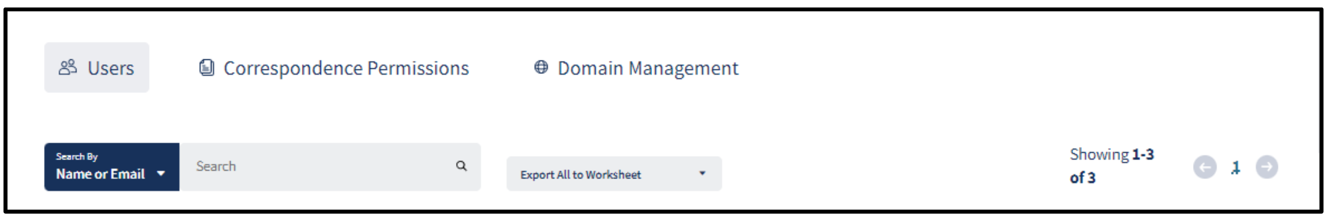


Figure 2.30: User Management.

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.

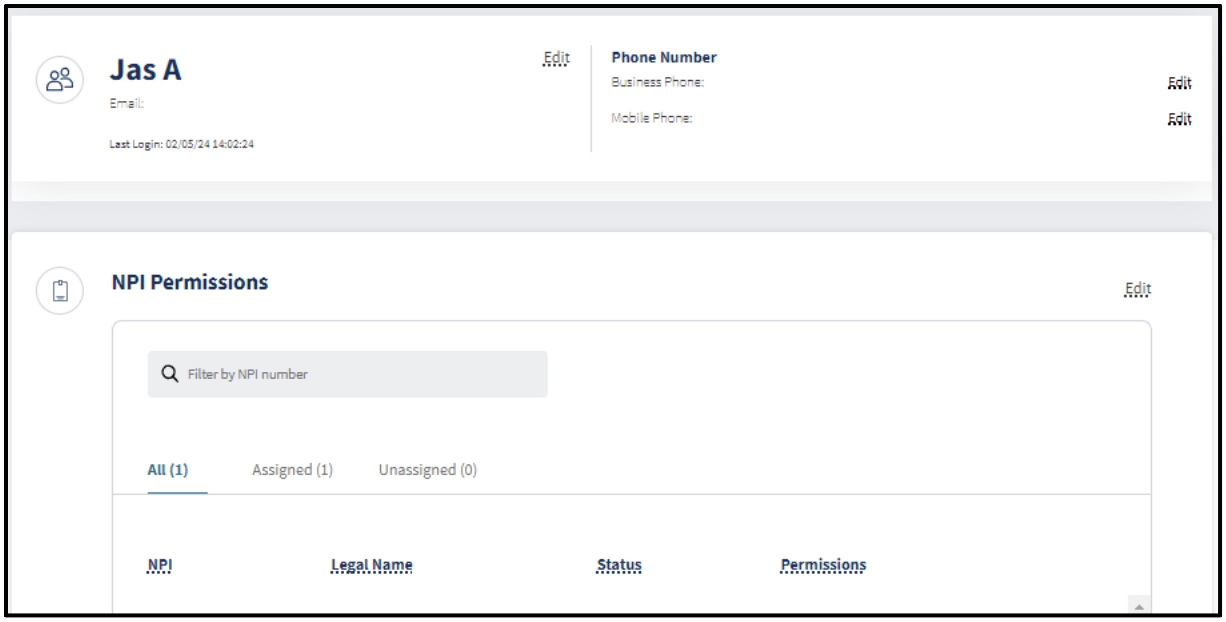


Figure 2.31: User Management and Permissions.

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.

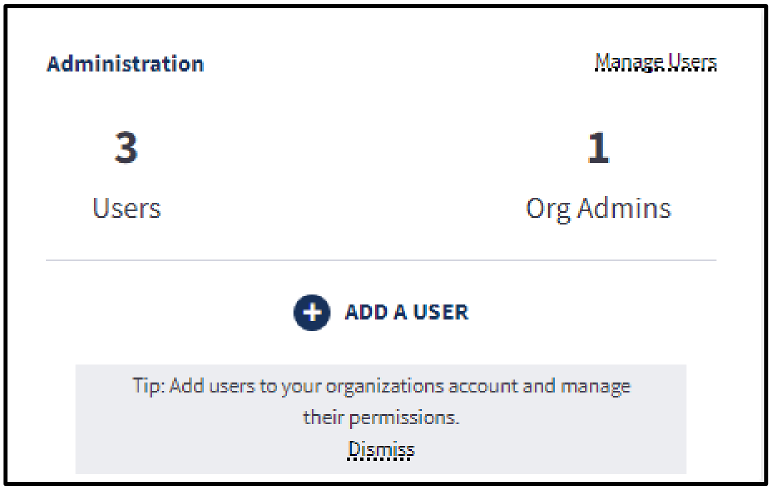


Figure 2.32: Administration Tile.

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

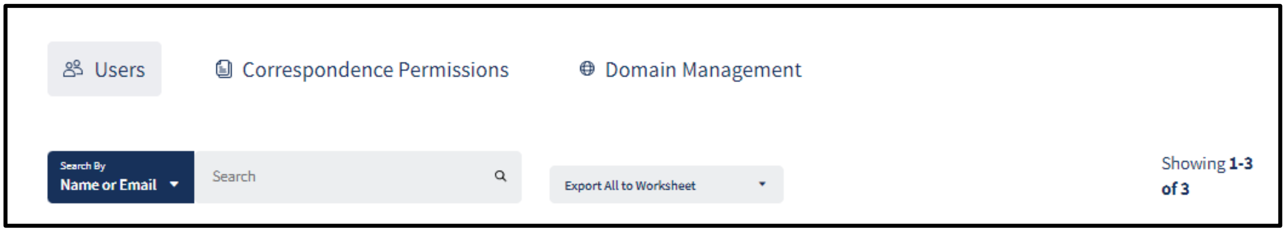


Figure 2.33: User Management.

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.

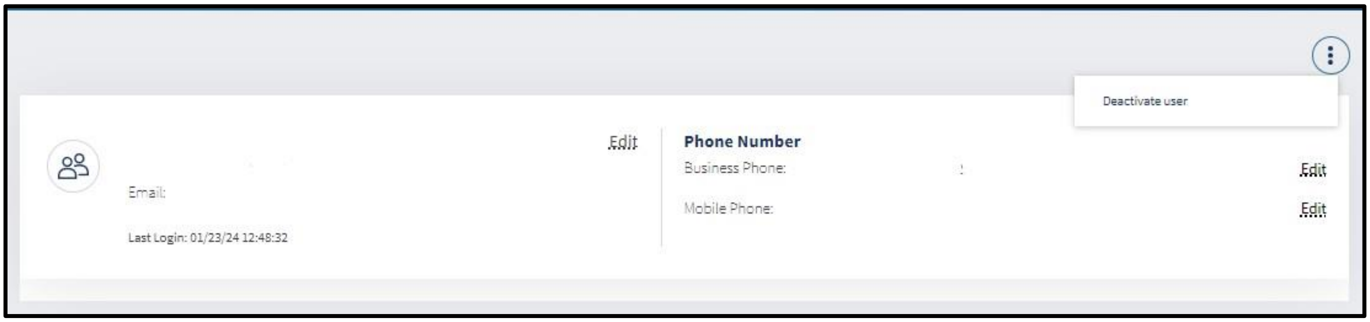


Figure 2.34: Deactivate User.

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

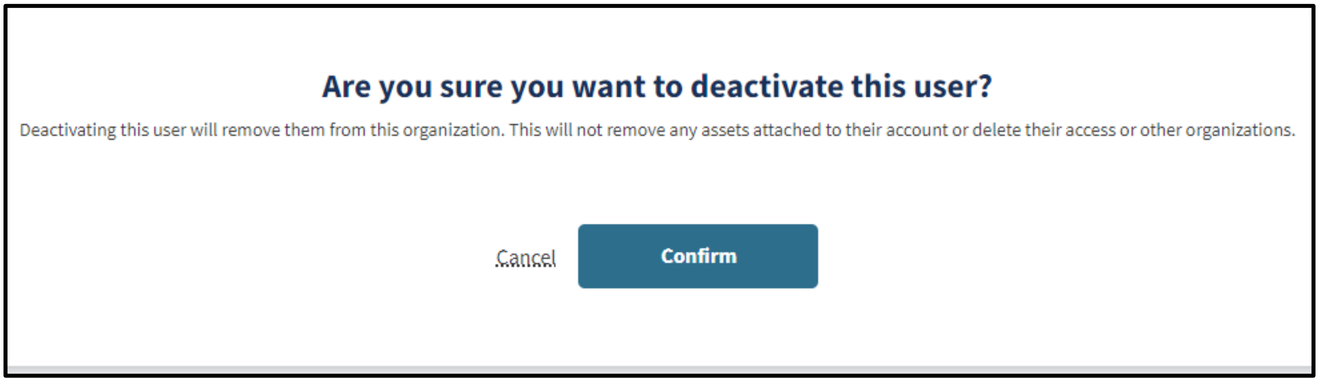


Figure 2.35: Confirmation to Deactivate User.

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.

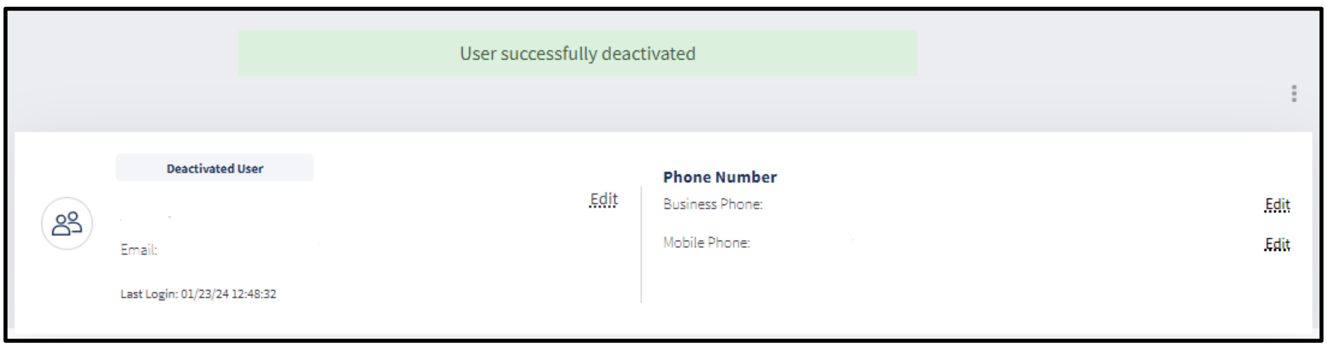


Figure 2.36: Deactivated User Messaging.

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.

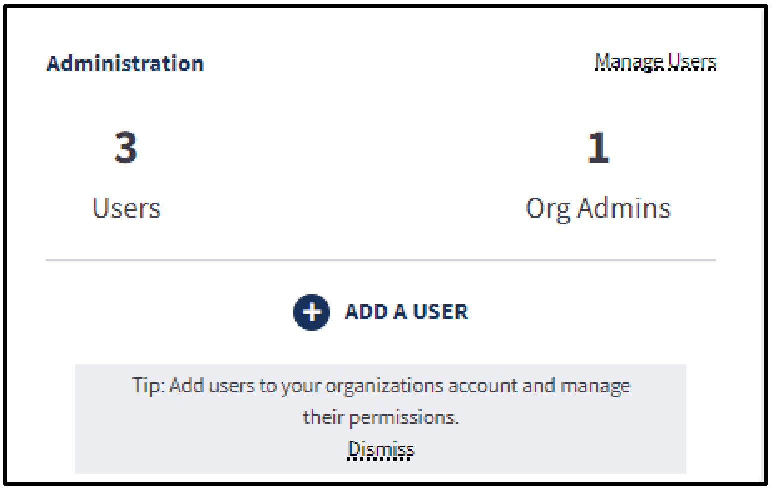


Figure 2.37: Administration Tile.

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

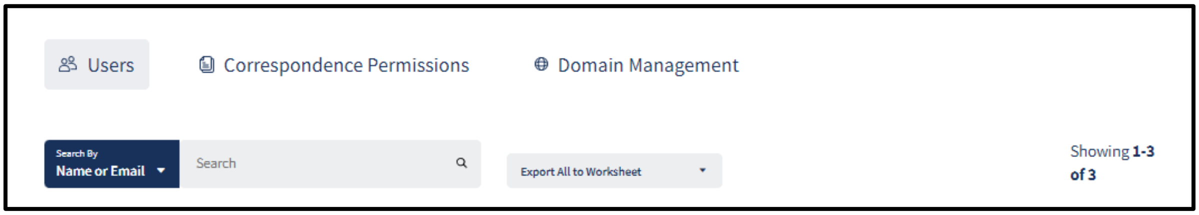


Figure 2.38: User Management.

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.

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

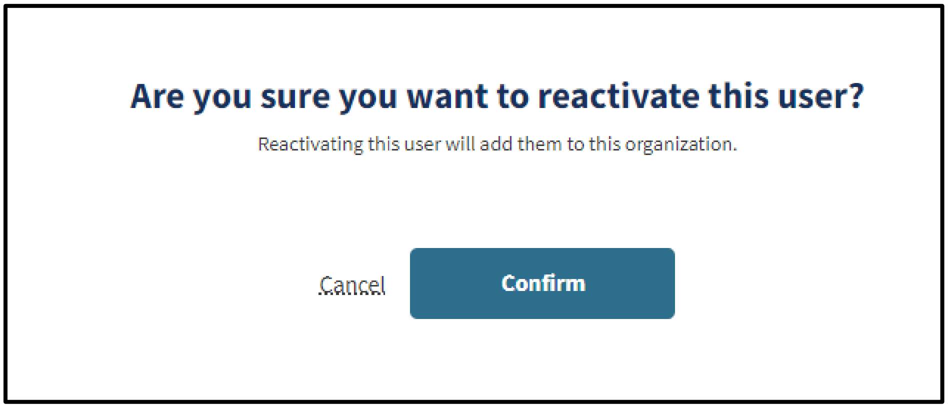


Figure 2.40: Reactivate User Confirmation.

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.

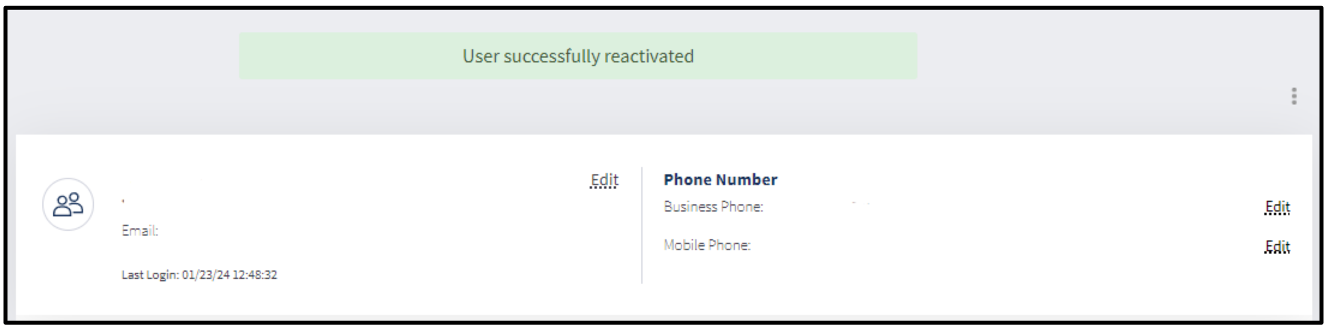


Figure 2.41: Reactivated User Messaging.

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.**

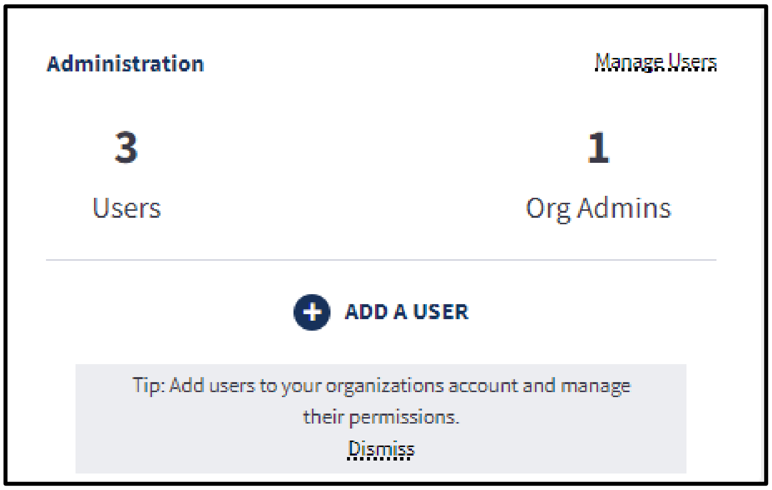


Figure 2.42: Administration Tile.

2. Click **Domain Management**.

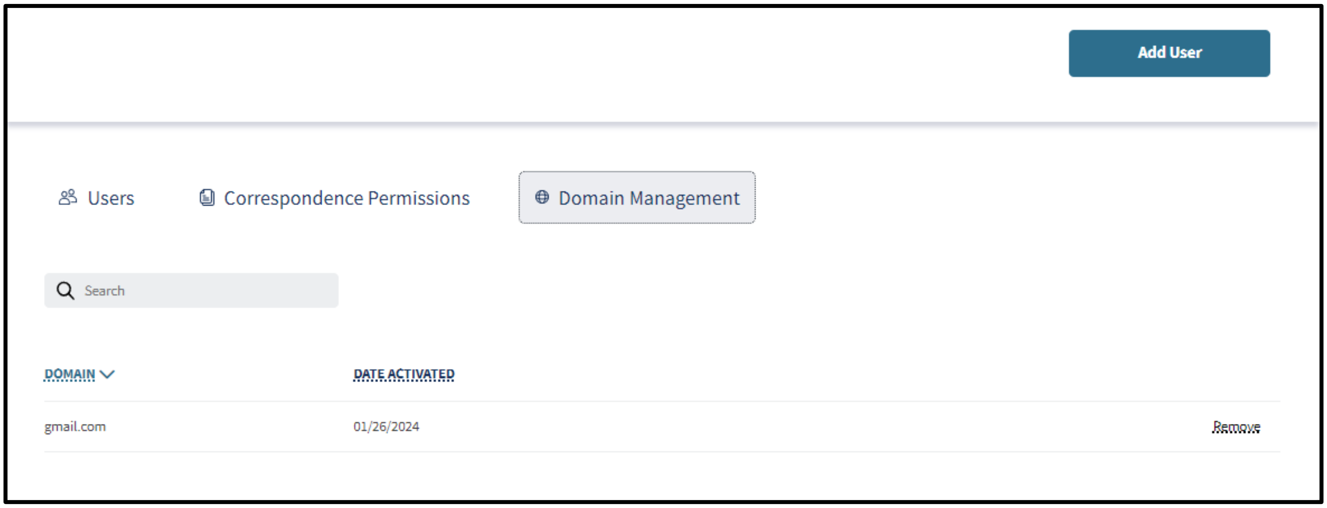


Figure 2.43: Domain Management.

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

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**.

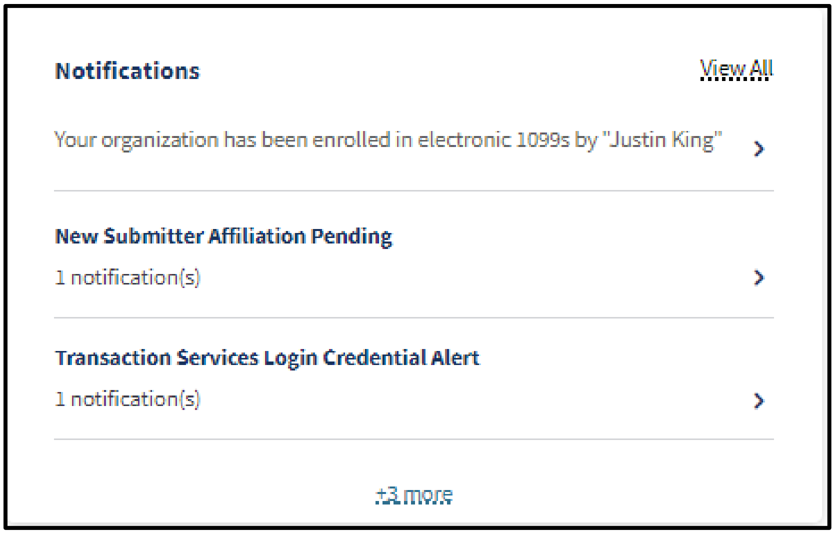


Figure 2.44: Notifications Tile.

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.

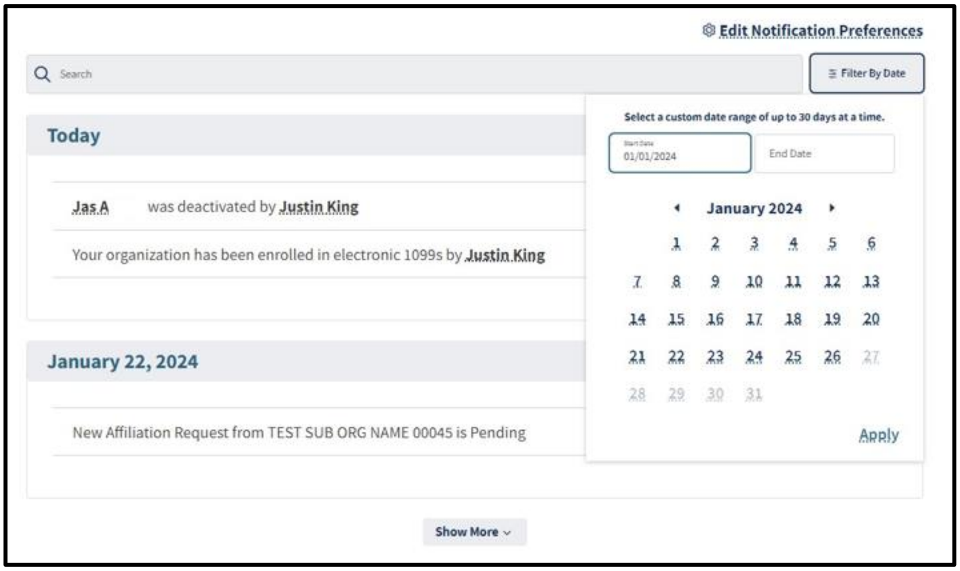


Figure 2.45: Filter by date for Notifications.

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.

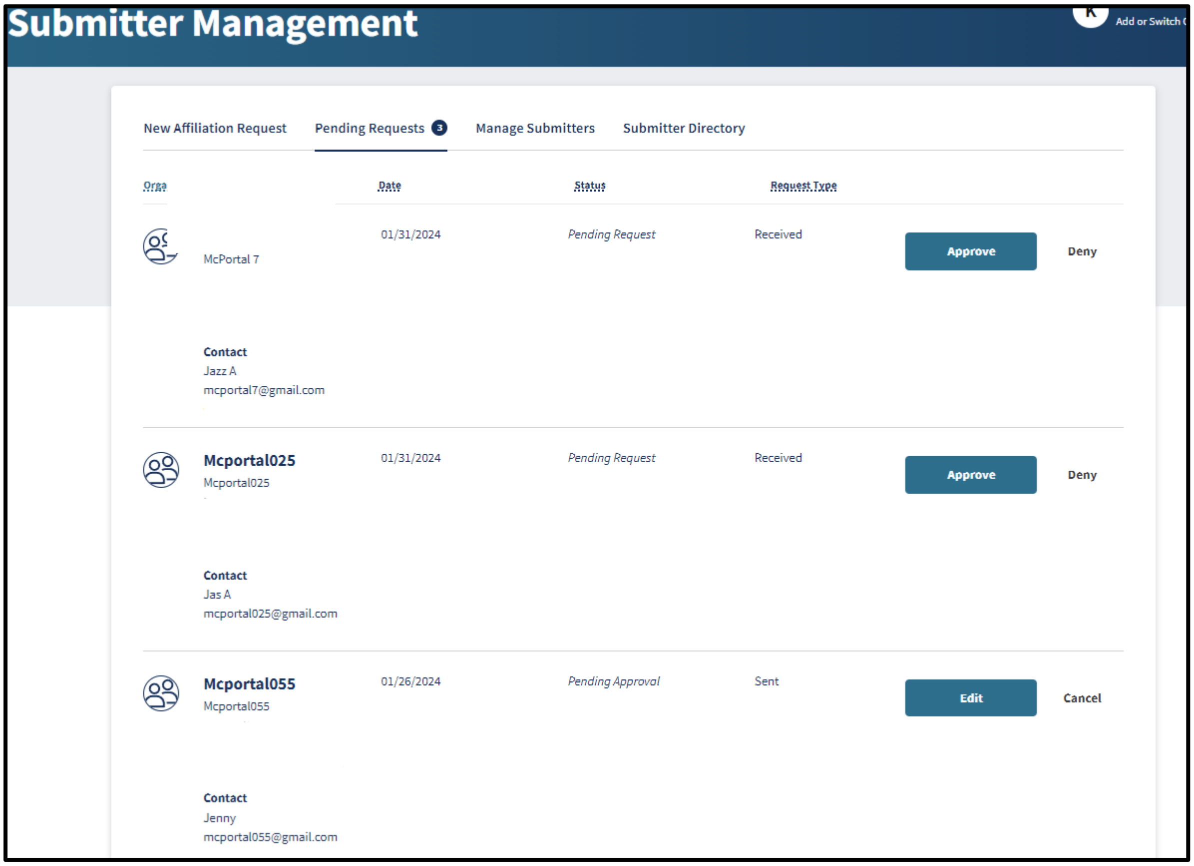


Figure 2.46: Pending Requests.

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.

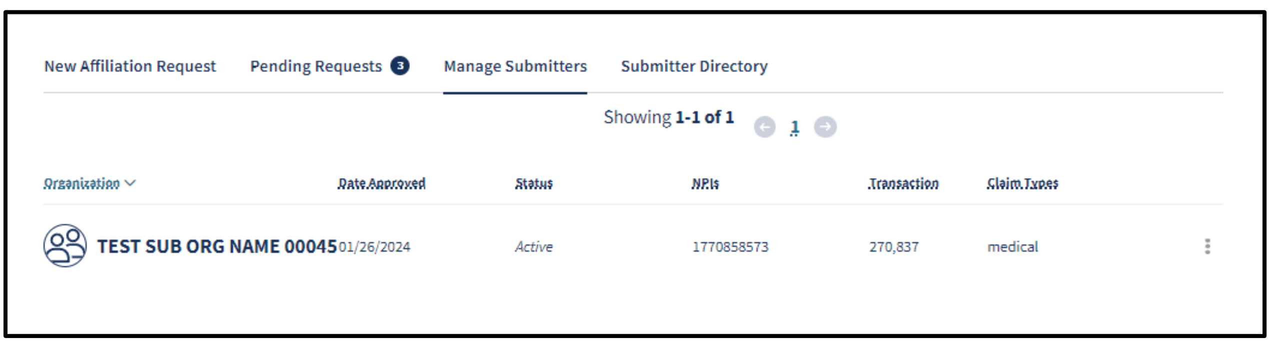


Figure 2.47: Manage Submitters.

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.

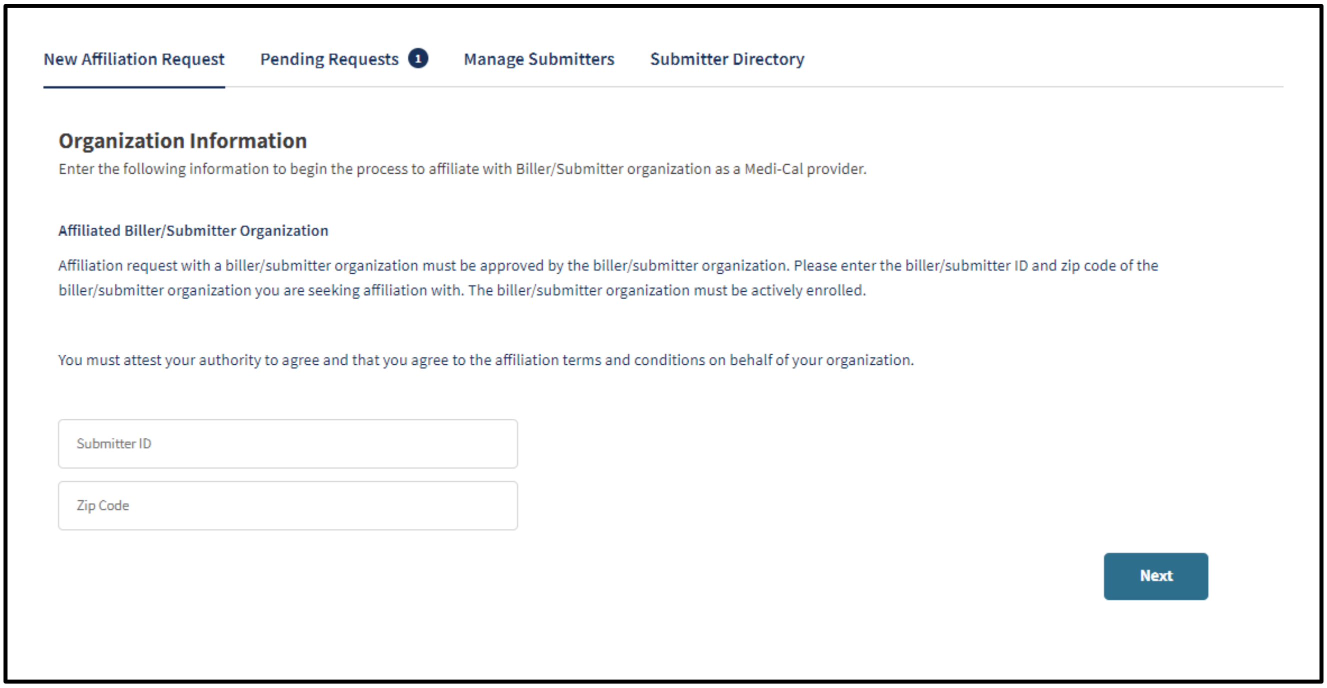


Figure 2.48: New Affiliation Request.

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.

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**.

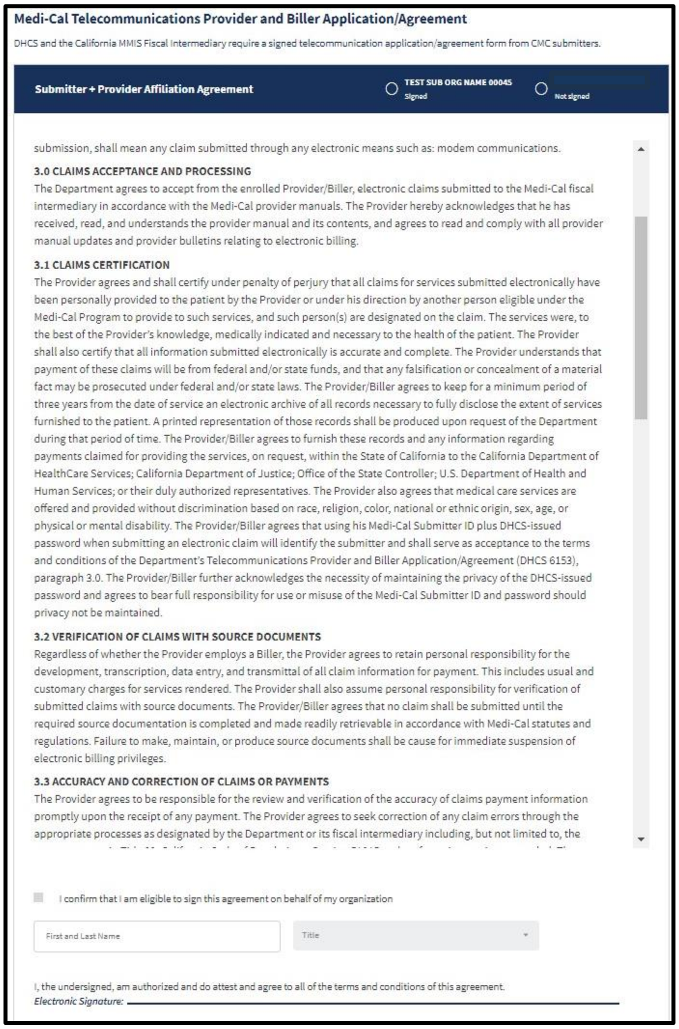


Figure 2.49: Medi-Cal Telecommunications Provider and Biller Application/Agreement.

3. A request complete screen will appear.

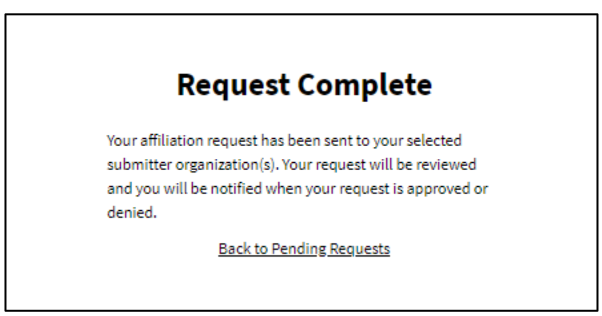


Figure 2.50: Request Complete.

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.

Approve a Submitter Affiliation Request

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

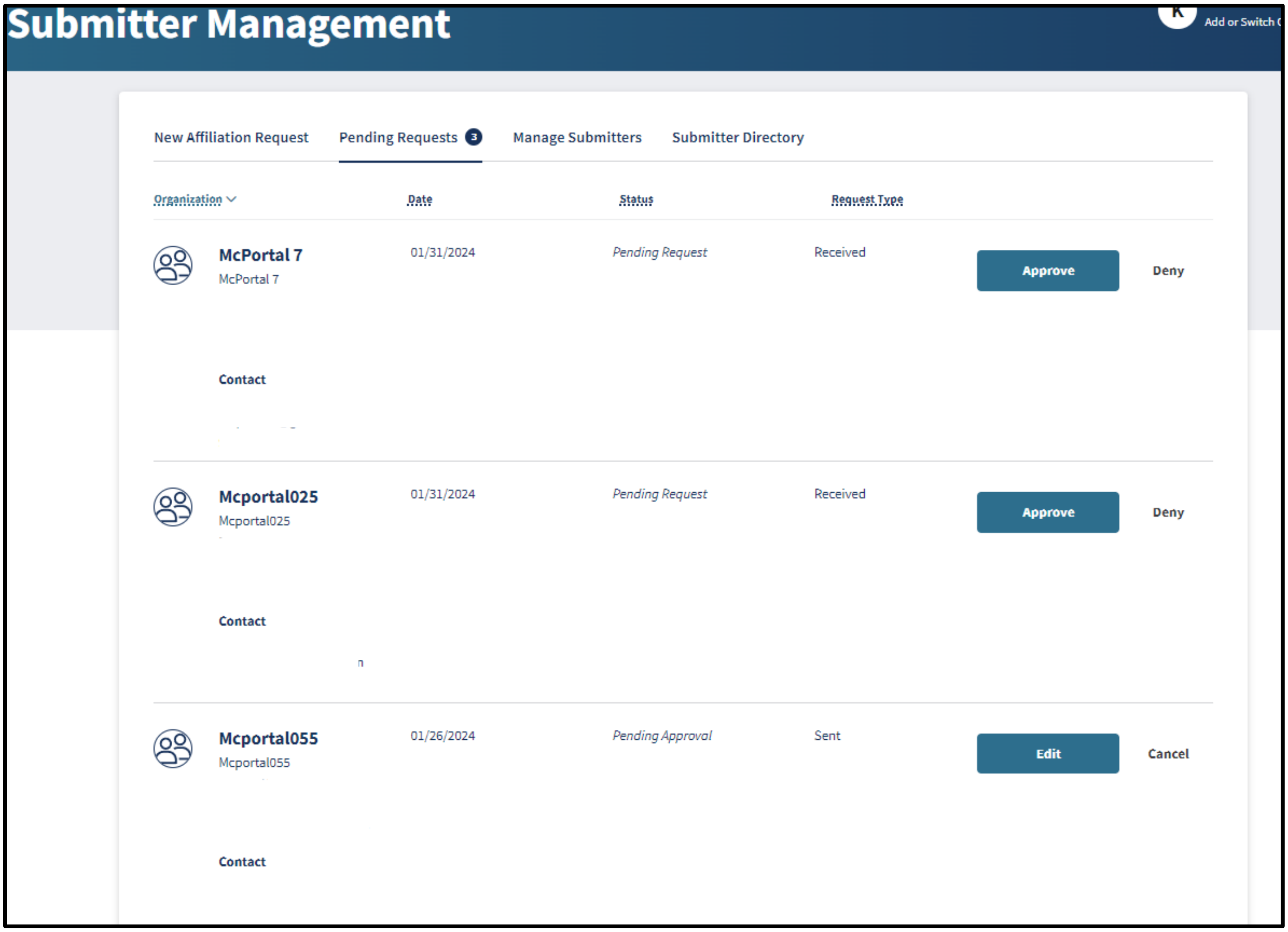


Figure 2.52: Pending Requests.

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

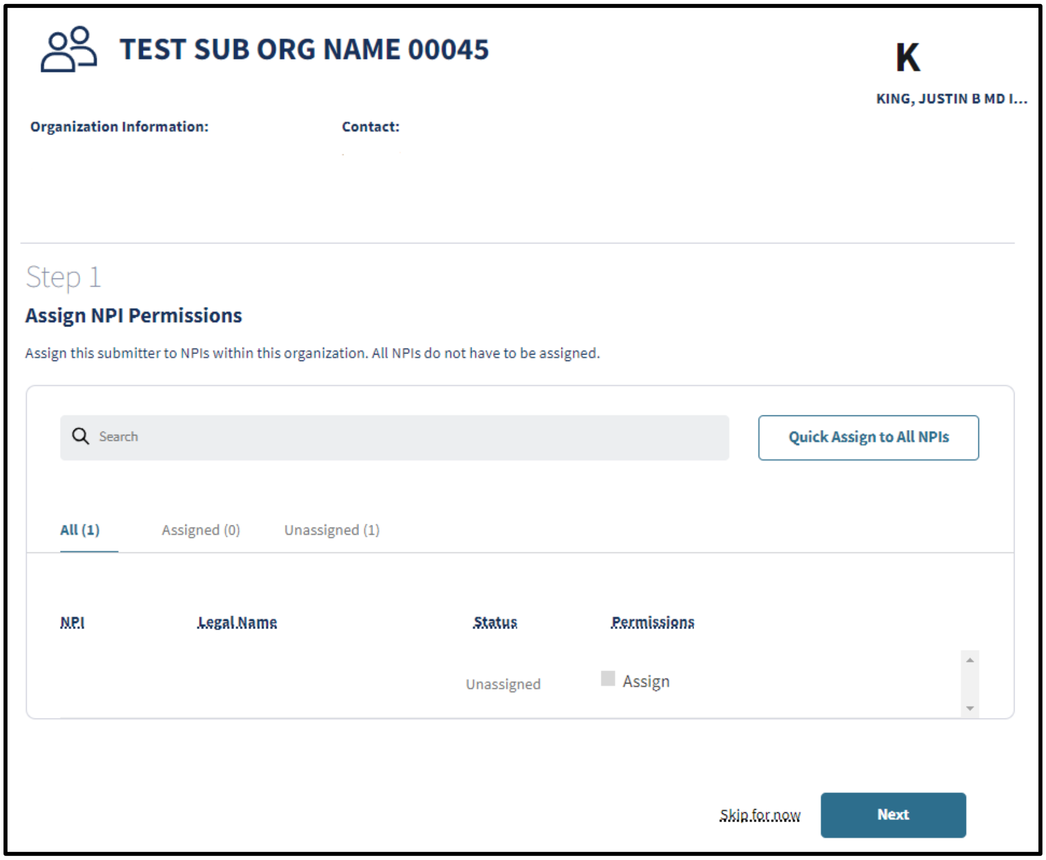


Figure 2.53: Step 1 Assign NPI Permissions.

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**.

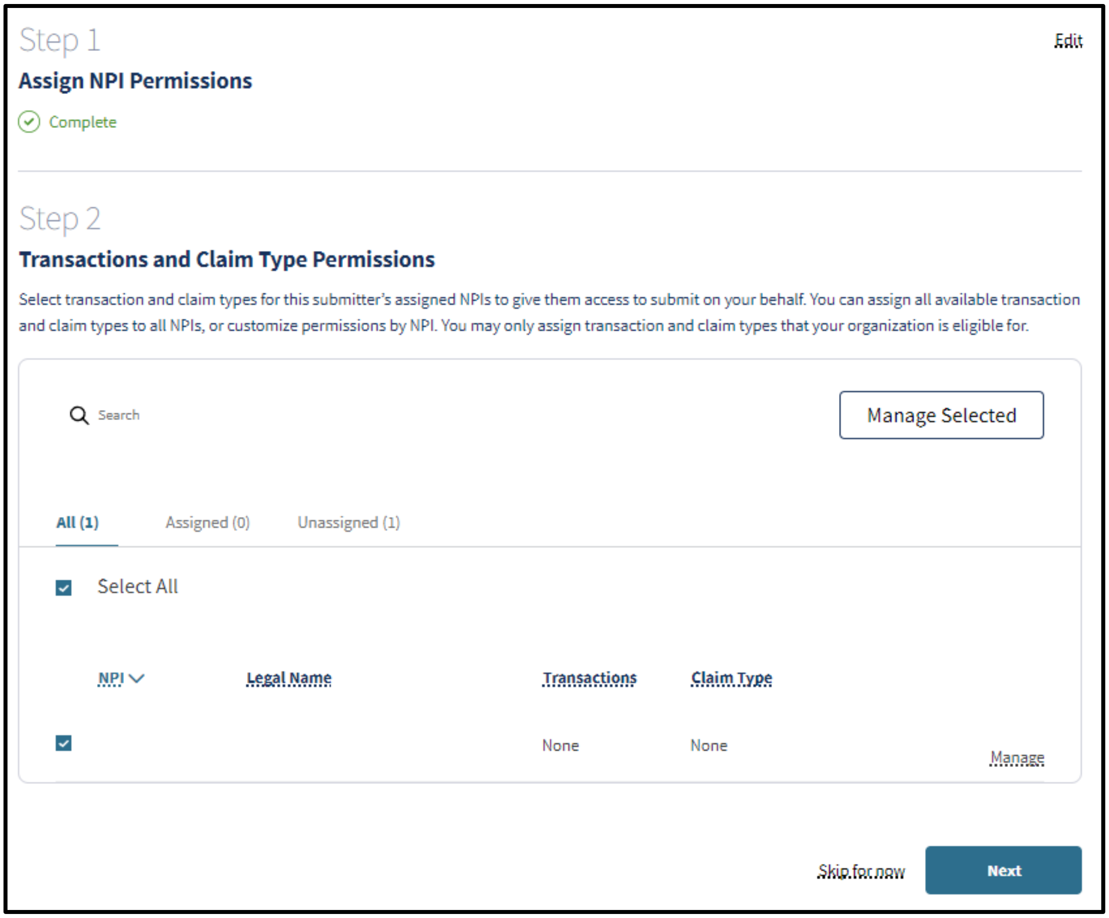


Figure 2.54: Step 2 Transactions and Claim Type Permissions.

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**.

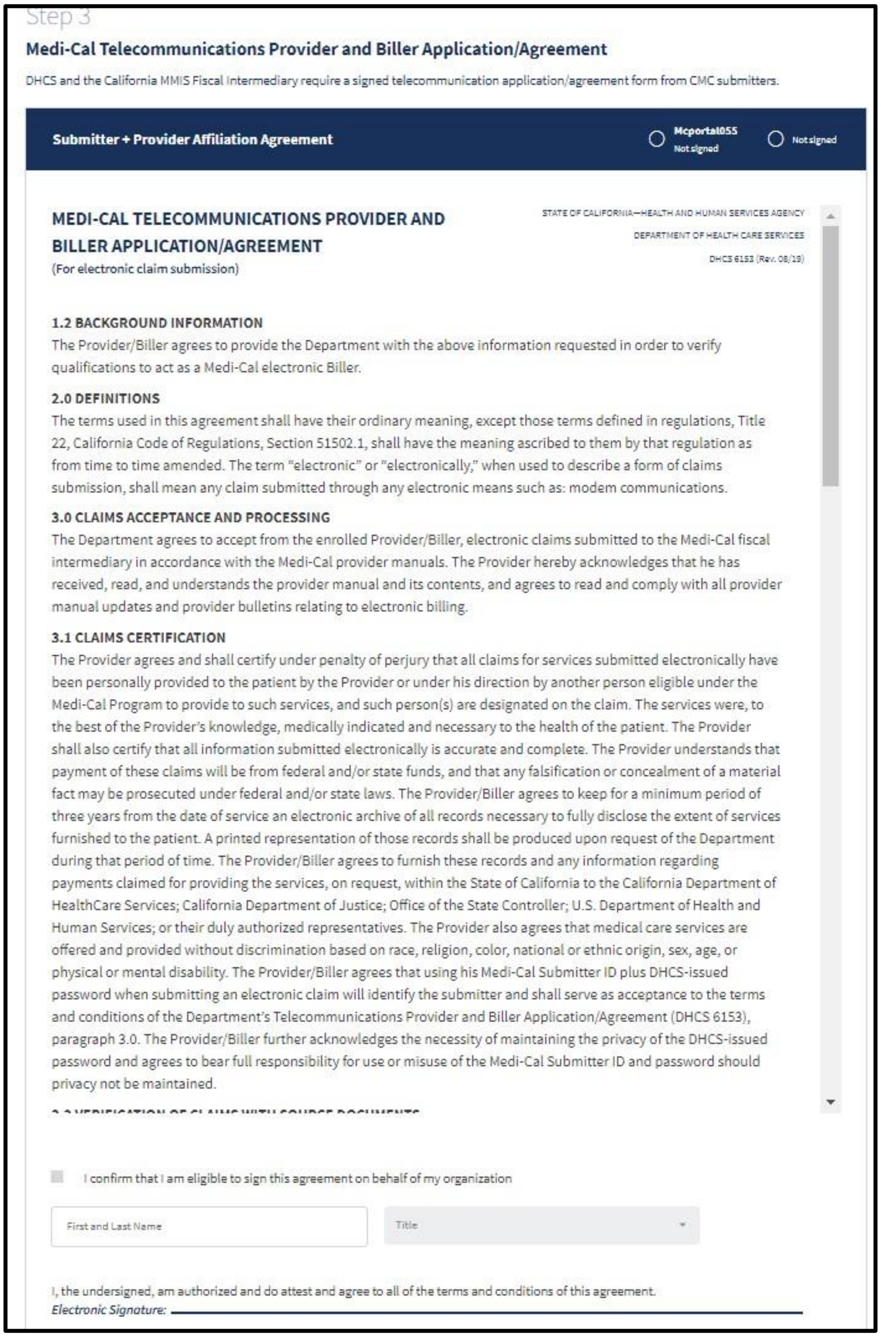


Figure 2.55: Step 3 Medi-Cal Telecommunications Provider and Biller Application/Agreement.

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

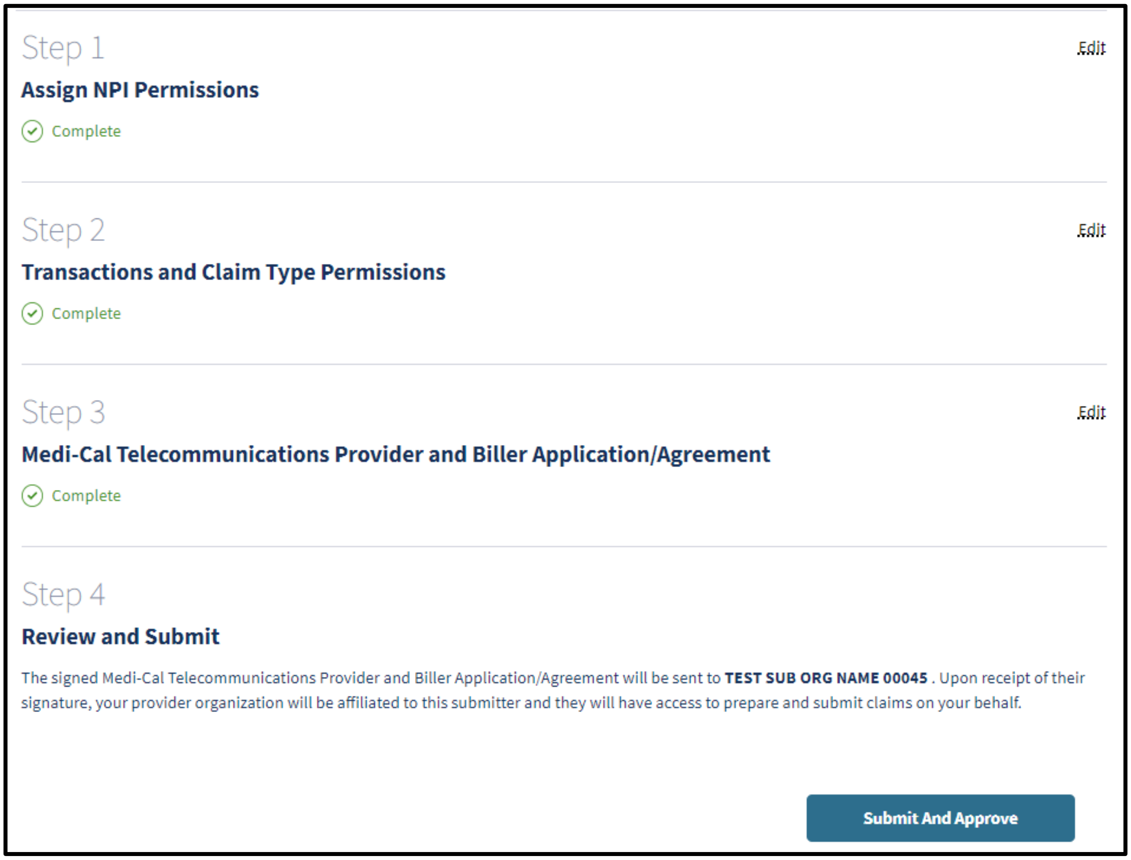


Figure 2.56: Step 4 Review and Submit.

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

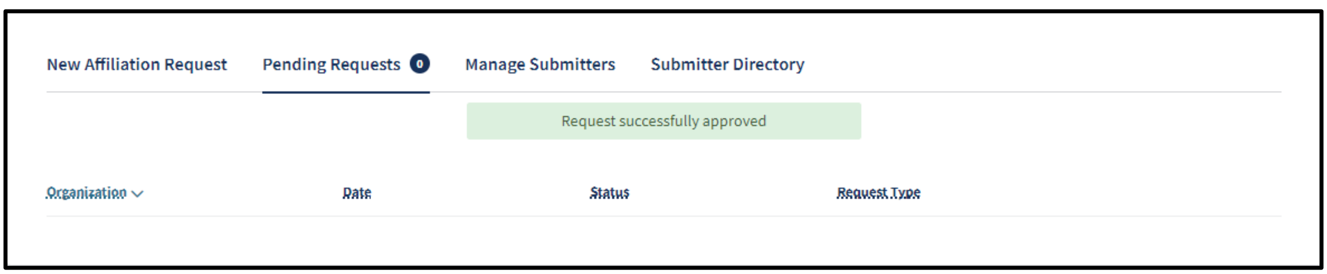


Figure 2.57: Request successfully approved.

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.

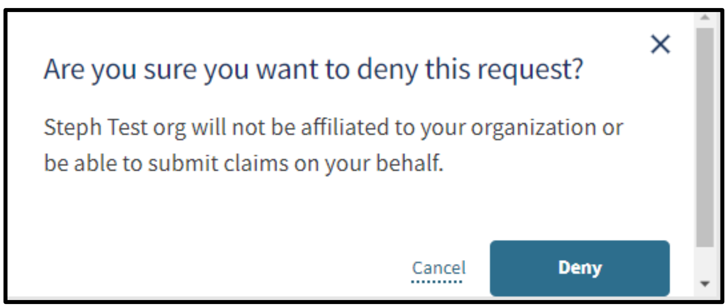


Figure 2.59: Deny Request Confirmation.

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

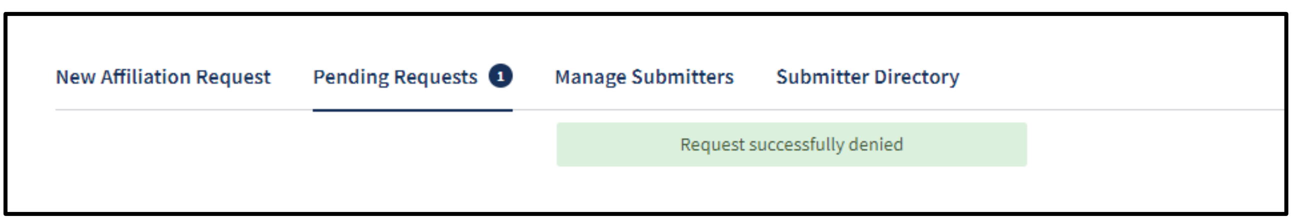


Figure 2.60: Request Successfully Denied.

Manage Submitters

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

Figure 2.61: Manage Submitters.

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

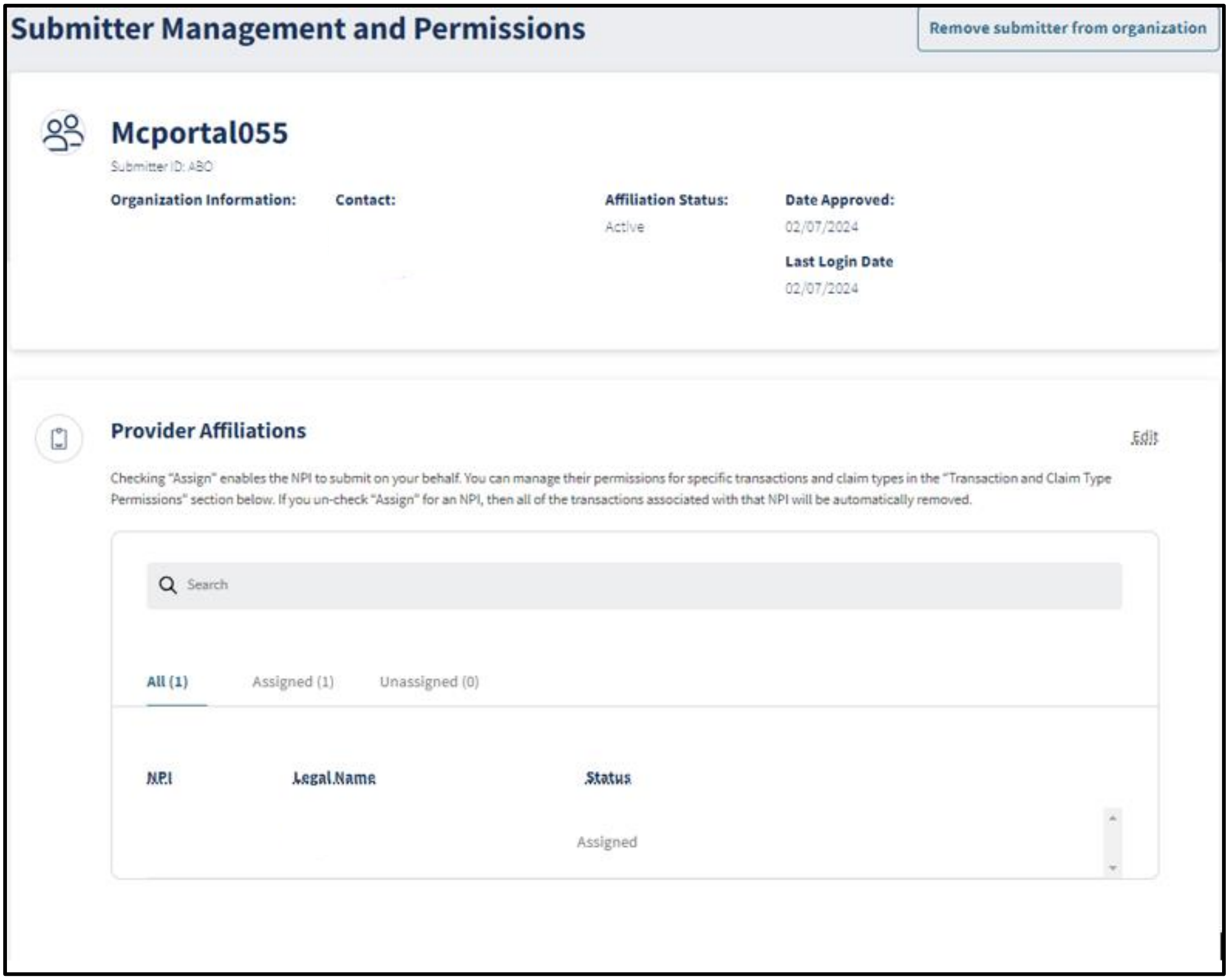


Figure 2.62: Submitter Management and Permissions.

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

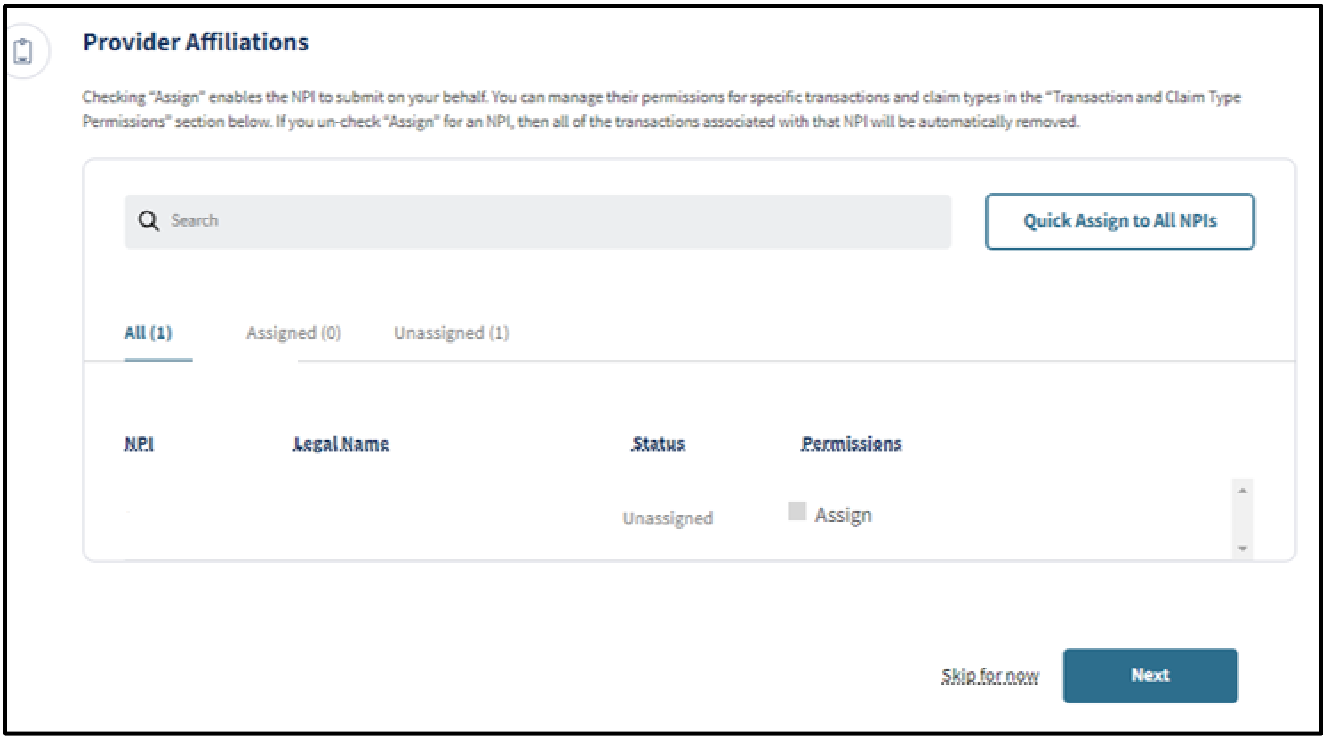


Figure 2.63: Provider Affiliations.

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

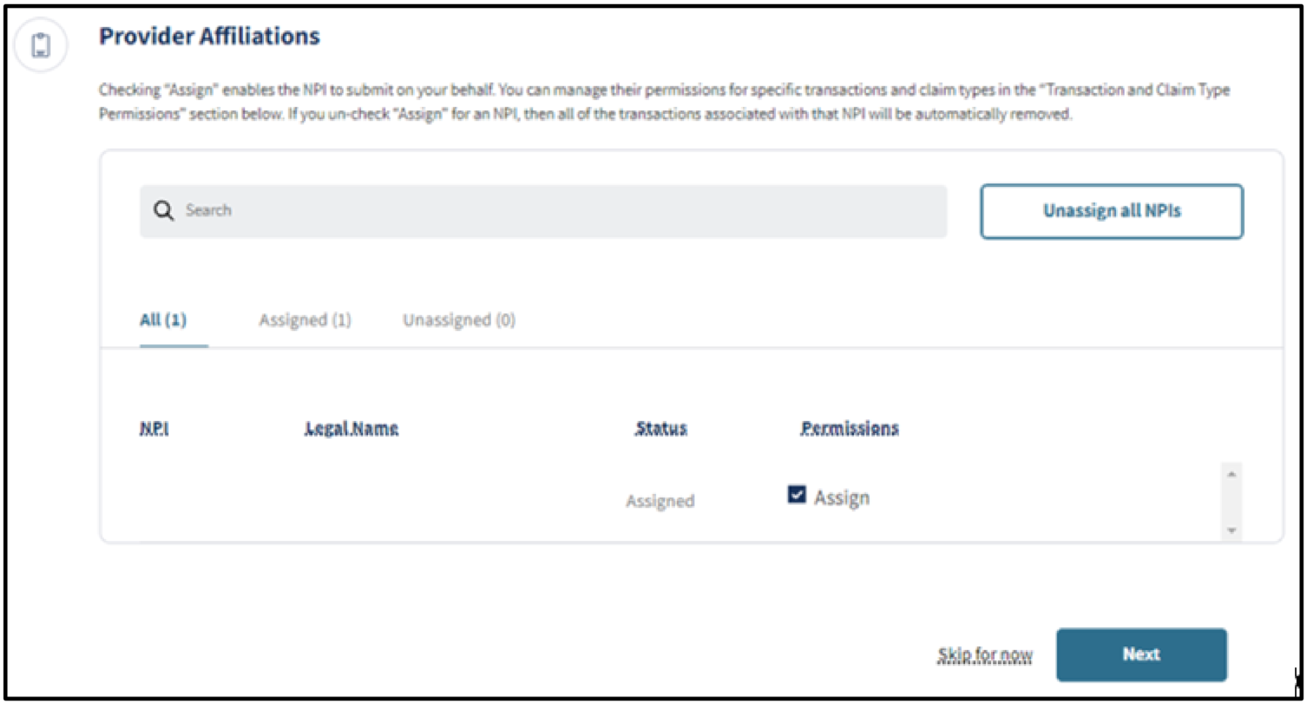


Figure 2.64: Assign NPI Permissions.

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

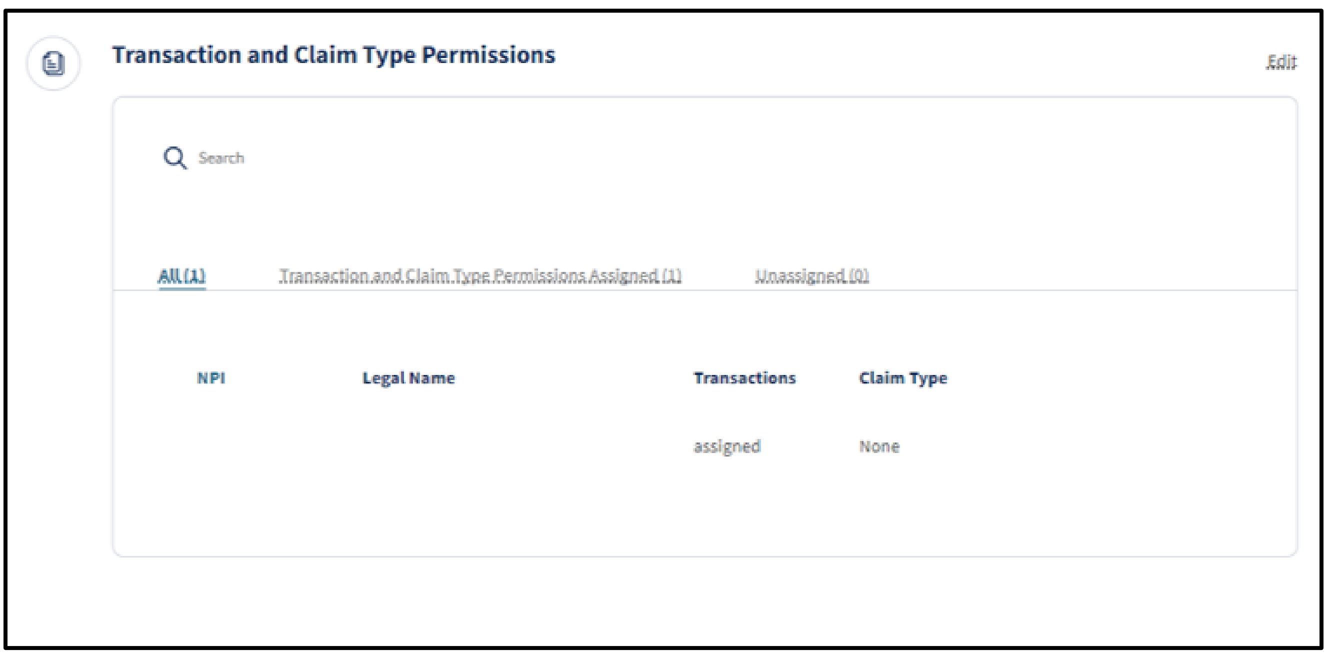


Figure 2.65: Transaction and Claim Type Permissions.

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

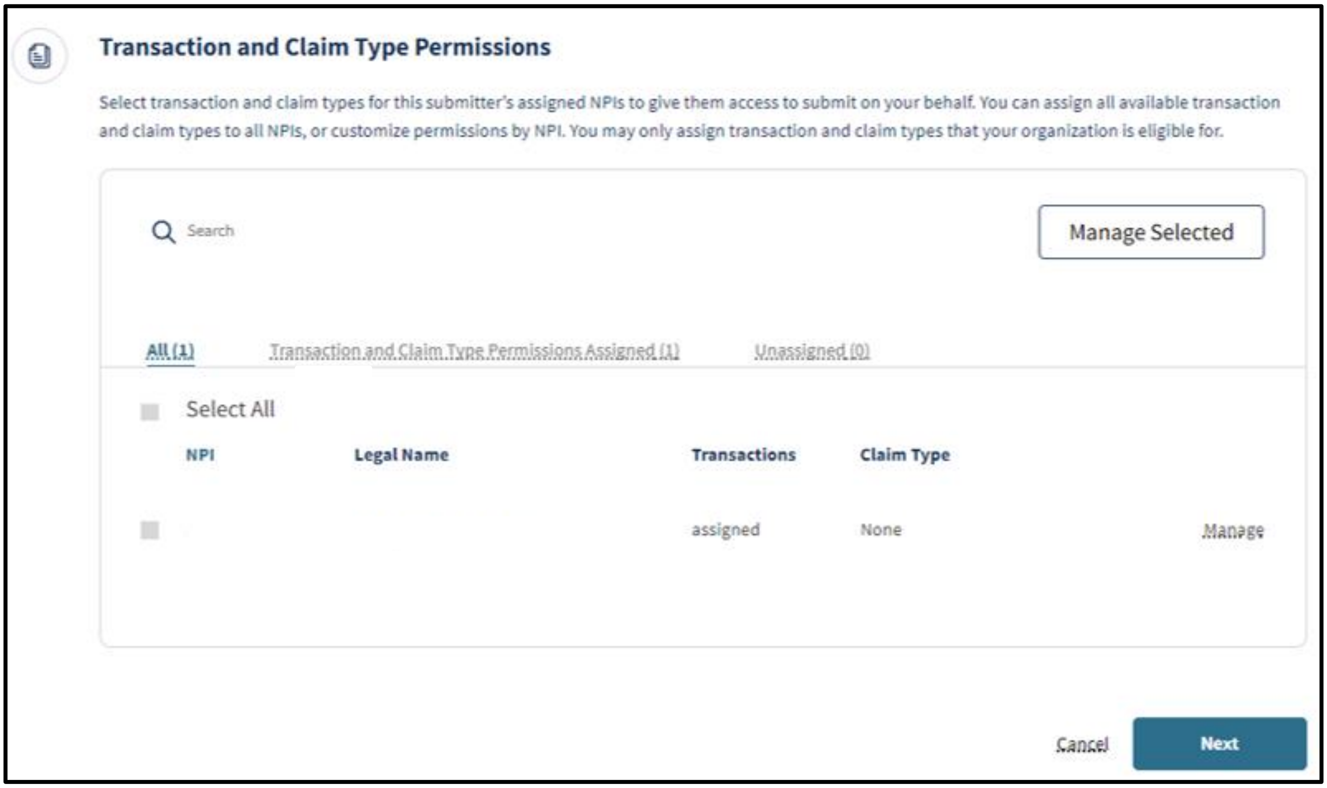


Figure 2.66: Manage Selected NPIs.

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

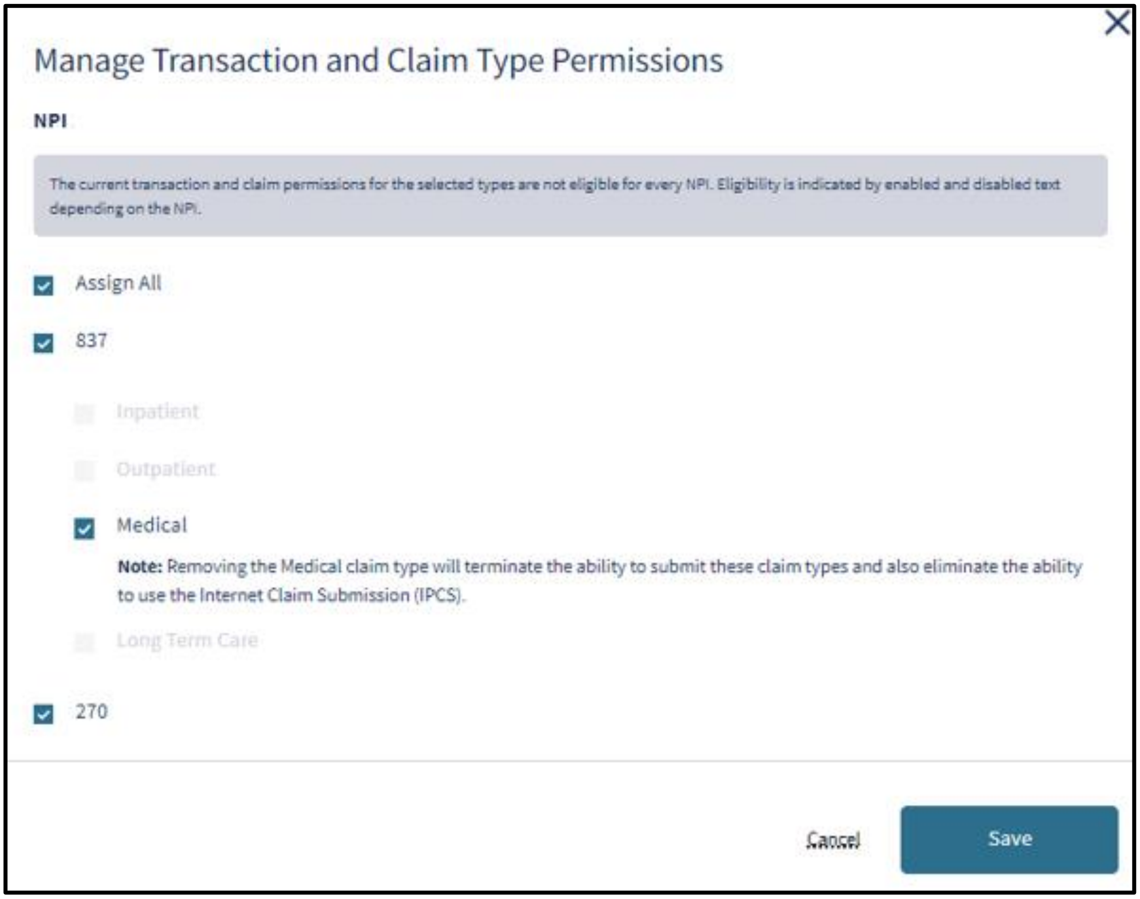


Figure 2.67: Manage Transaction and Claim Type Permissions.

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

Figure 2.68: View Signed Agreement and Signatures.

Submitter Directory

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

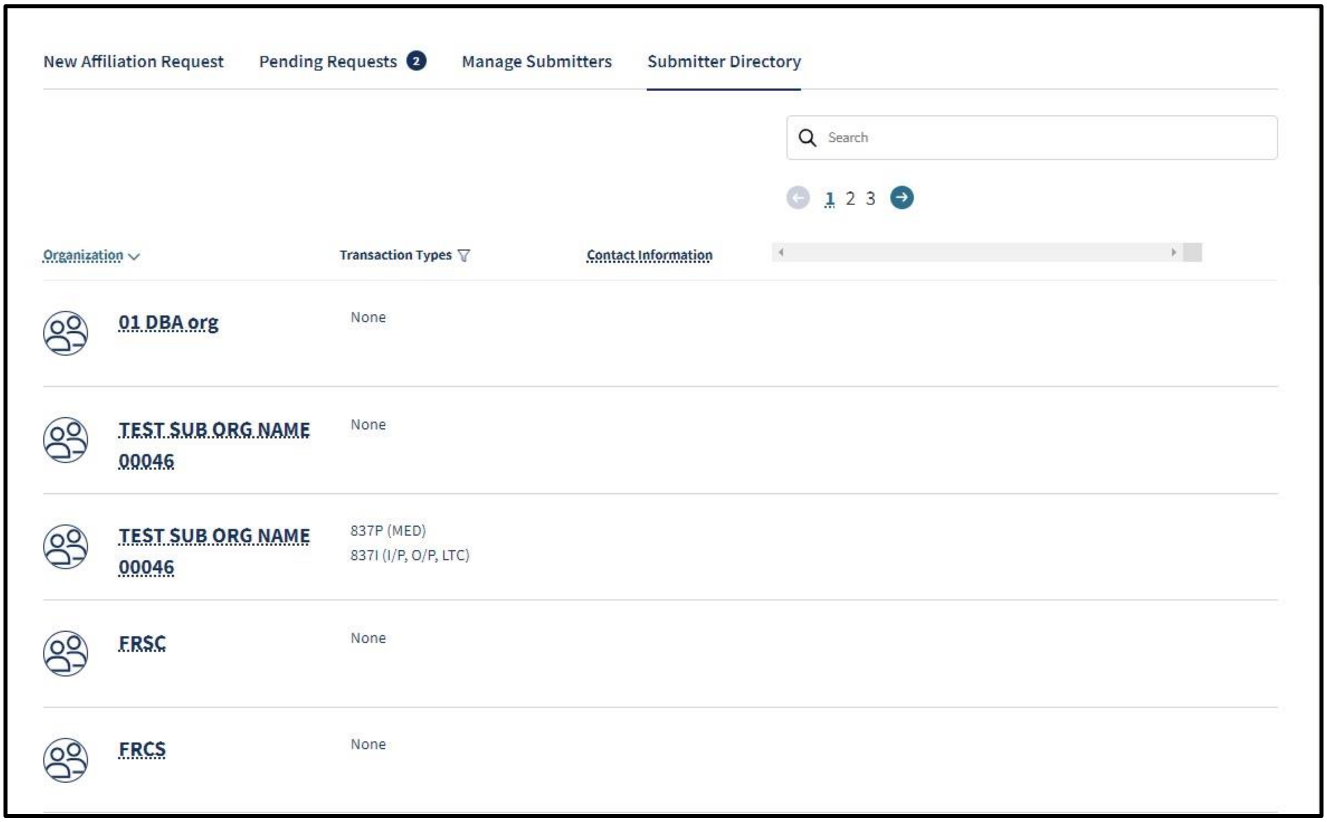


Figure 2.69: Submitter Directory.

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.

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.

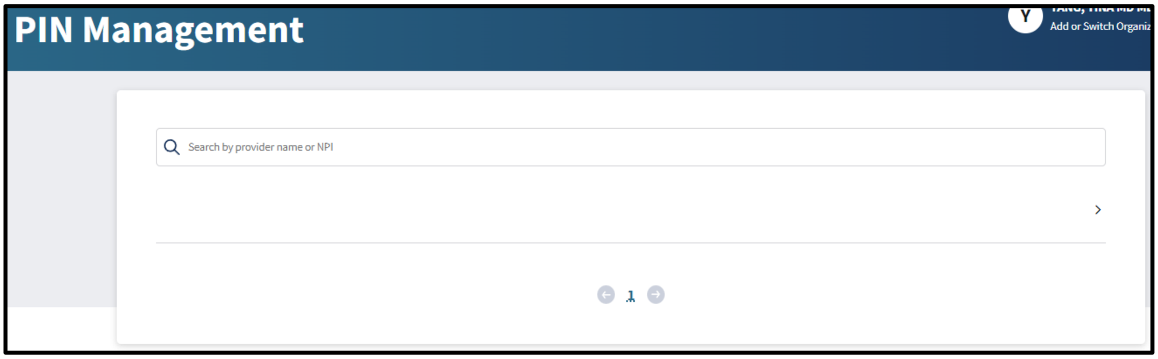


Figure 2.72: Search NPIs.

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

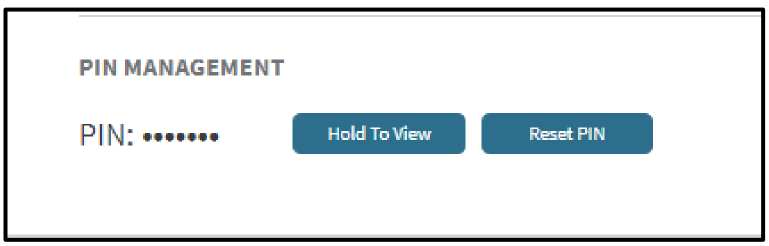


Figure 2.73: Hold to View or Reset PIN.

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.

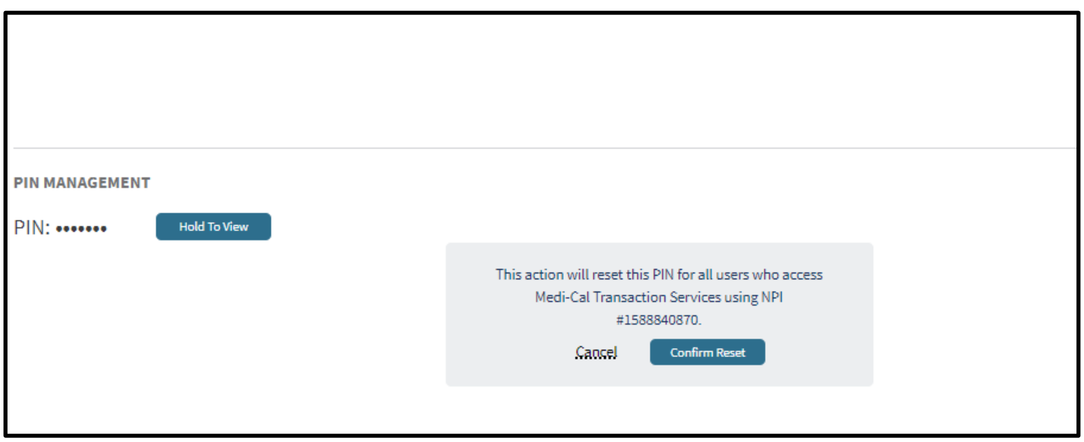


Figure 2.74: Confirm PIN Reset.

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

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**.

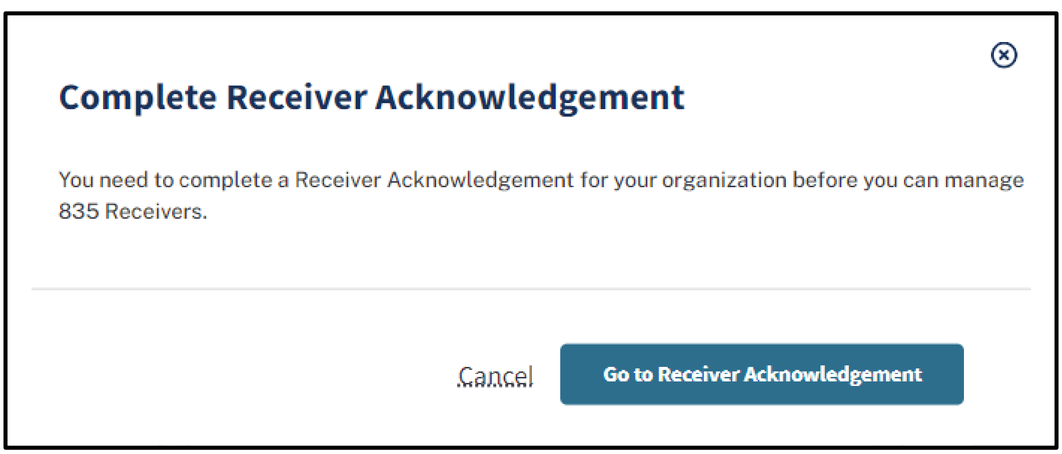


Figure 2.76: Complete Receiver Acknowledgement.

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**.

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

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

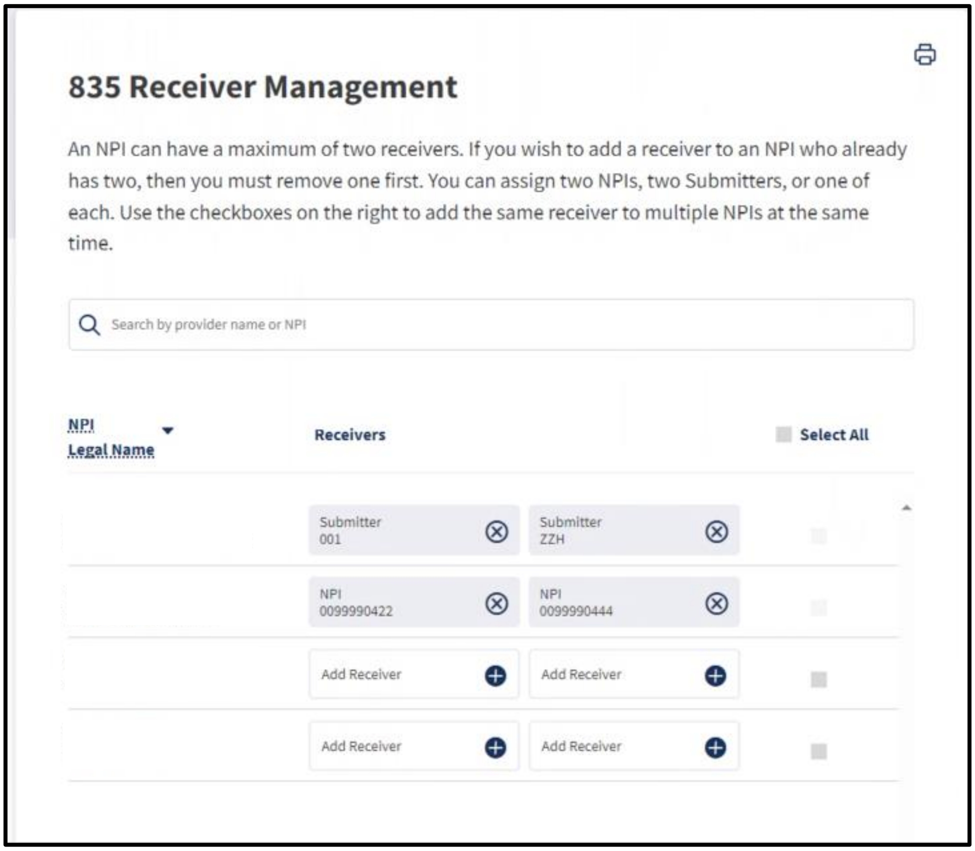


Figure 2.78: 835 Receiver Management.

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

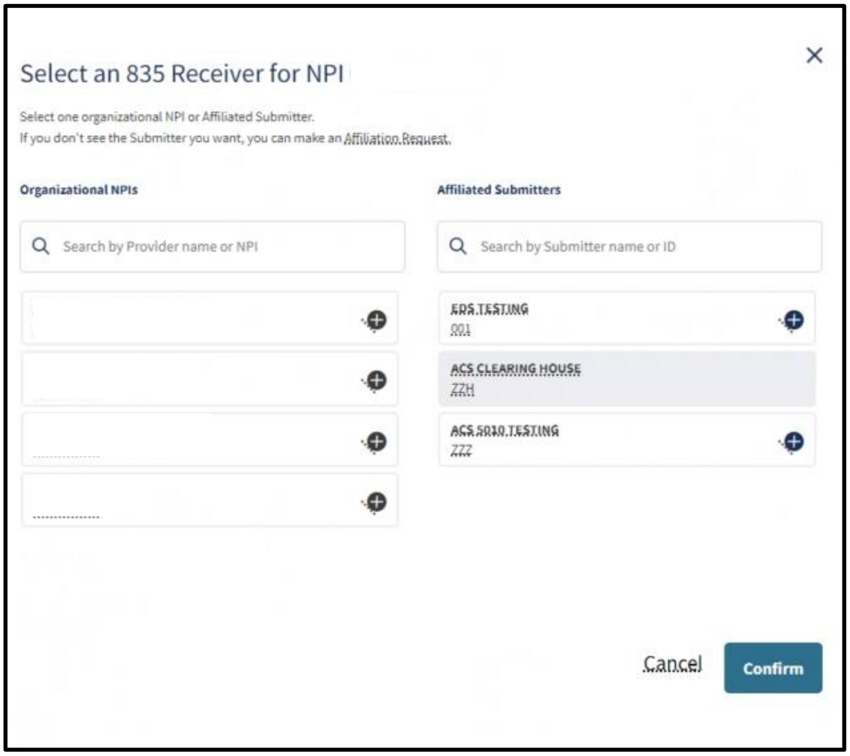


Figure 2.79: Select an 835 Receiver for NPI.

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.

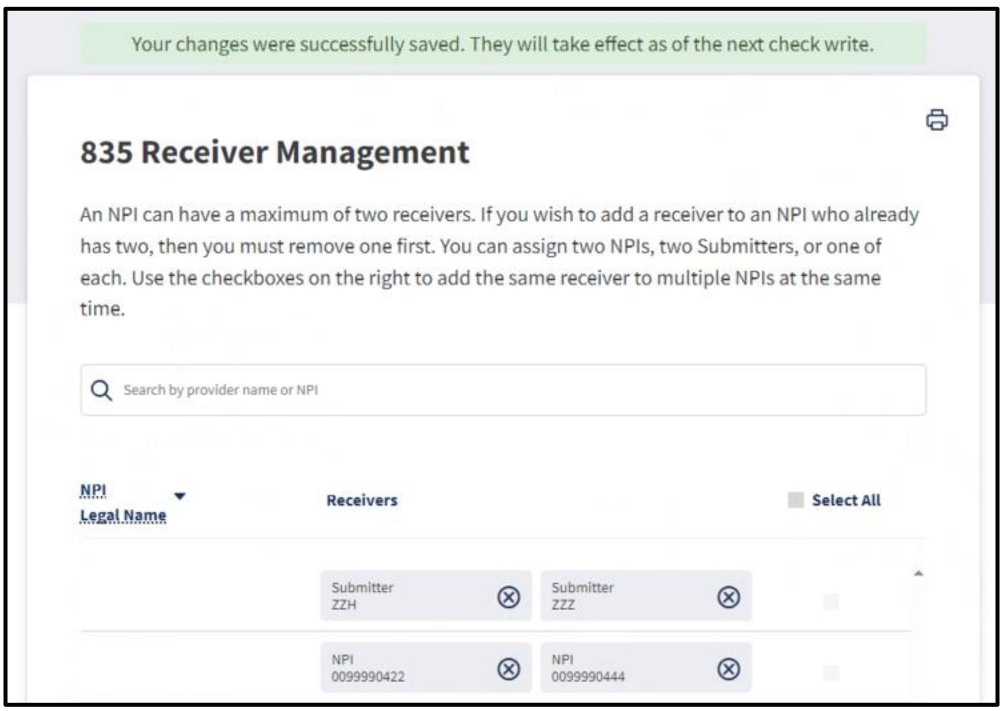


Figure 2.81: Successfully Added Receivers.

Remove 835 Receiver

1. Click the "**x**" symbol next to the receiver organization name.

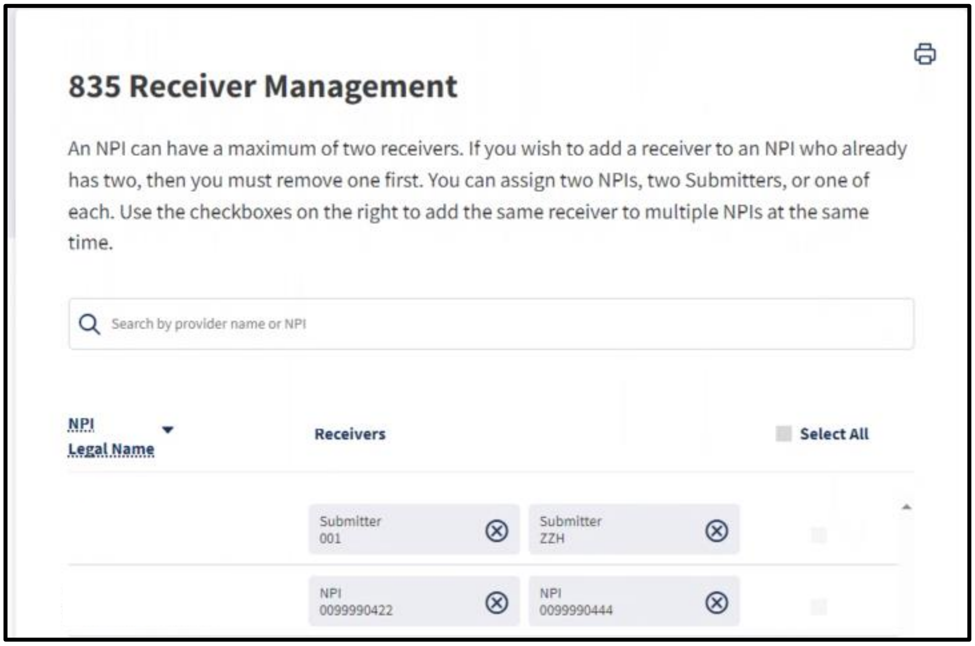


Figure 2.82: 835 Receiver Management.

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

Figure 2.83: Remove Receiver Confirmation.

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

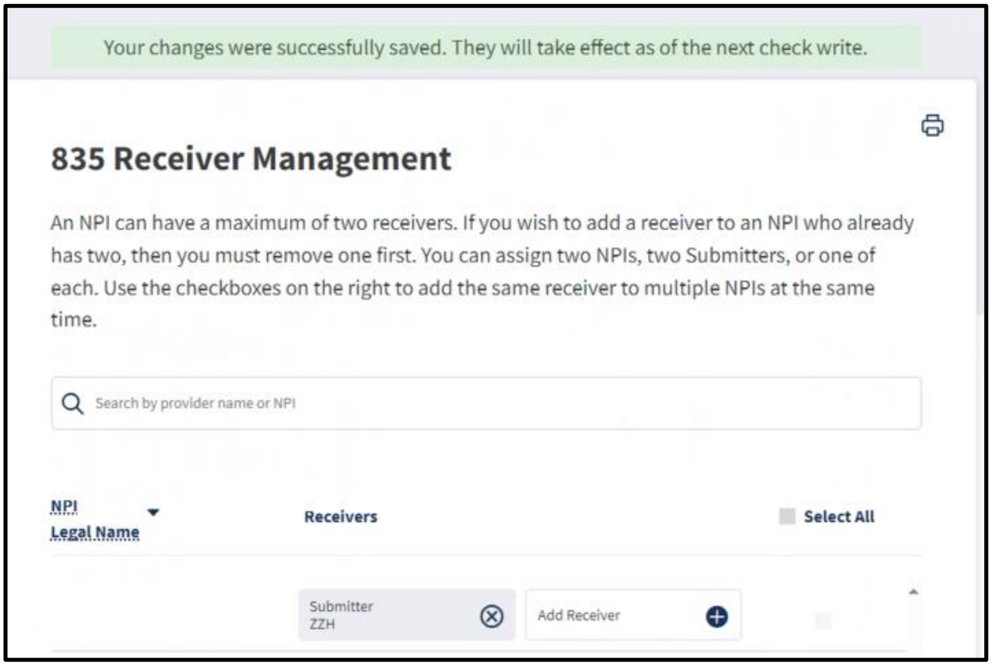


Figure 2.84: Successfully Removed Receiver.

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

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.

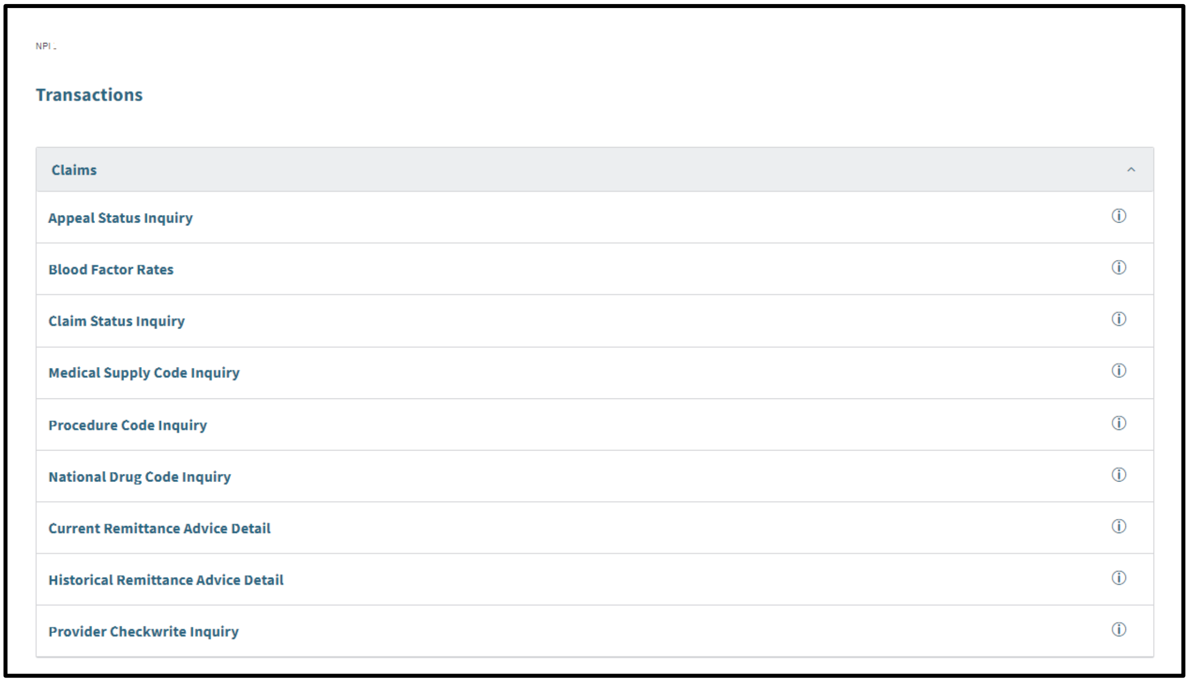


Figure 2.85: NPI Transactions List.

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

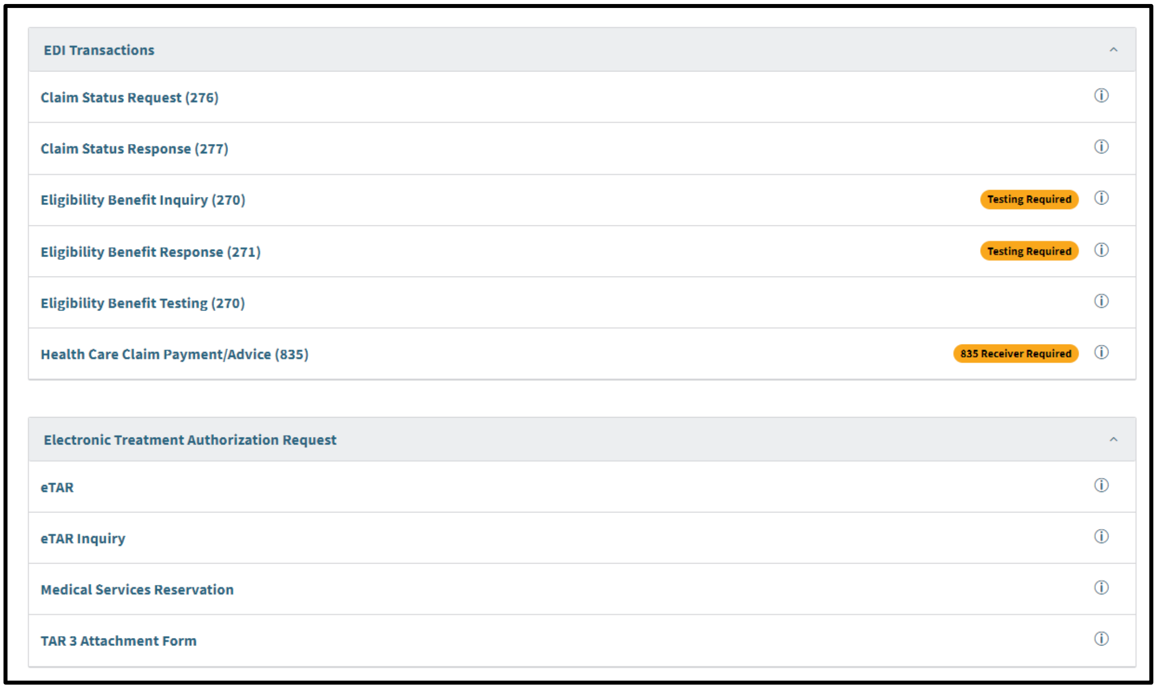


Figure 2.86: NPI Transactions List.

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.

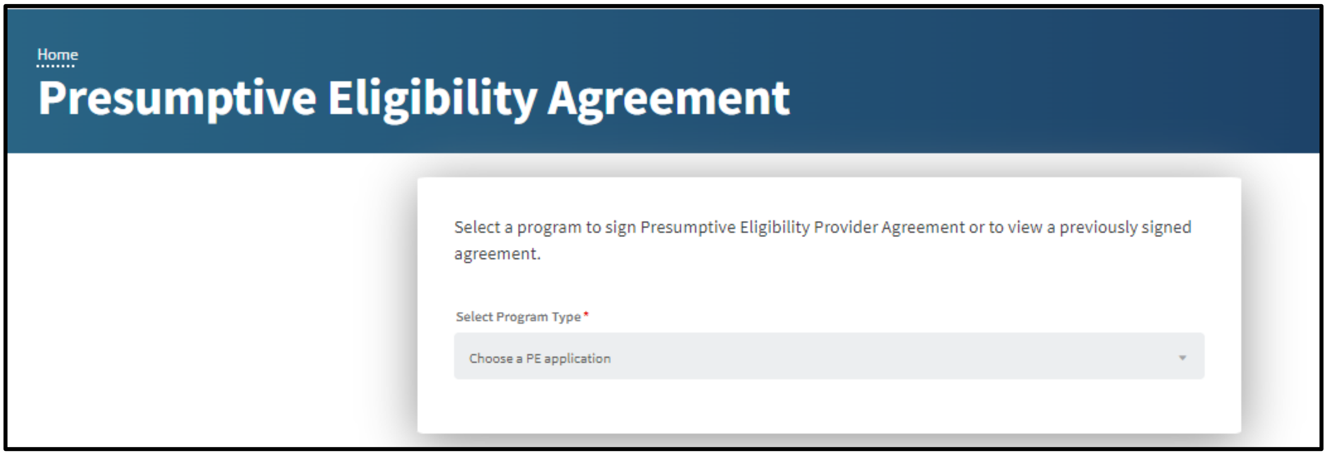


Figure 2.87: Select PE Program Type Drop-Down Menu.

Communication Center

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

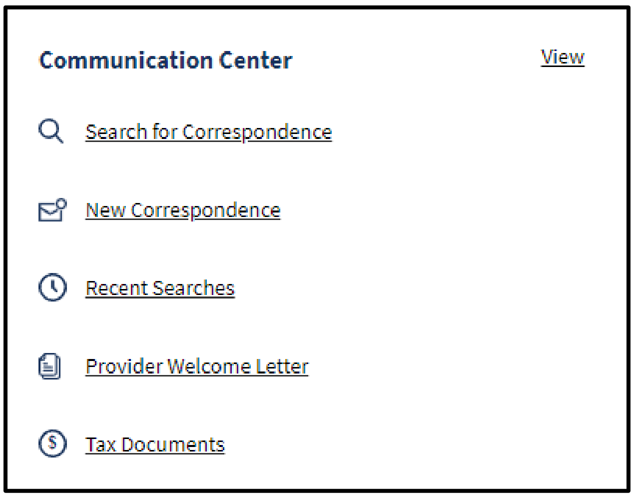


Figure 2.88: Communication Center Tile.

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

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.

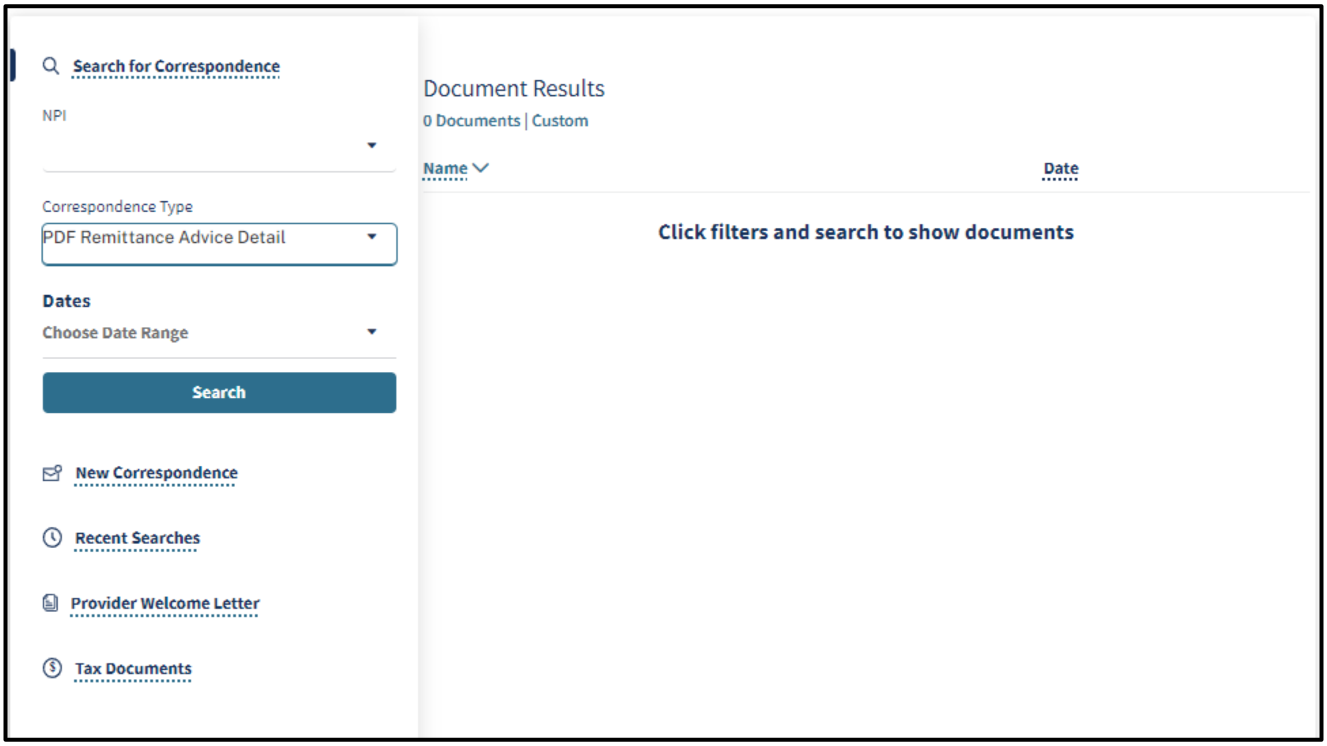


Figure 2.89: Search for Correspondence.

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.

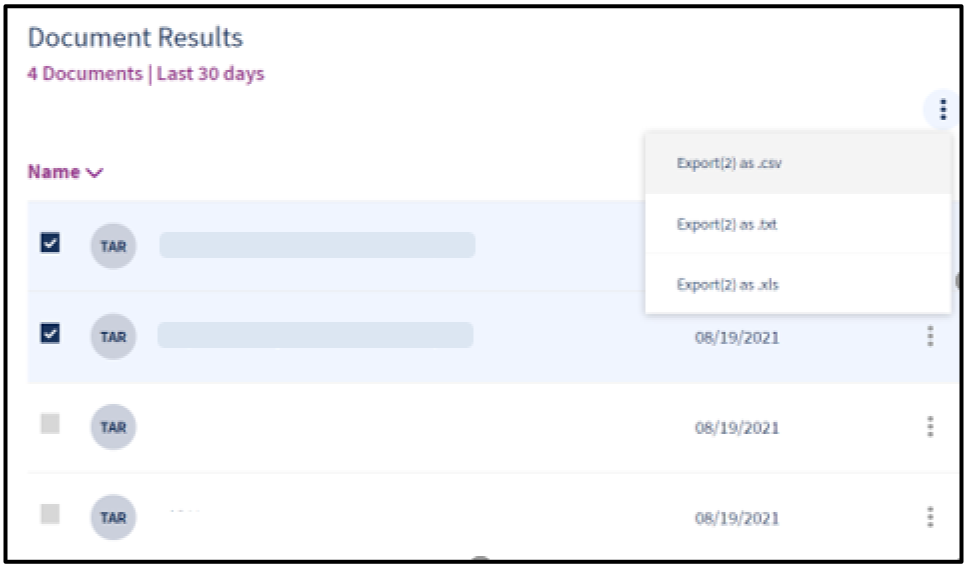


Figure 2.90: Document Results.

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.

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.

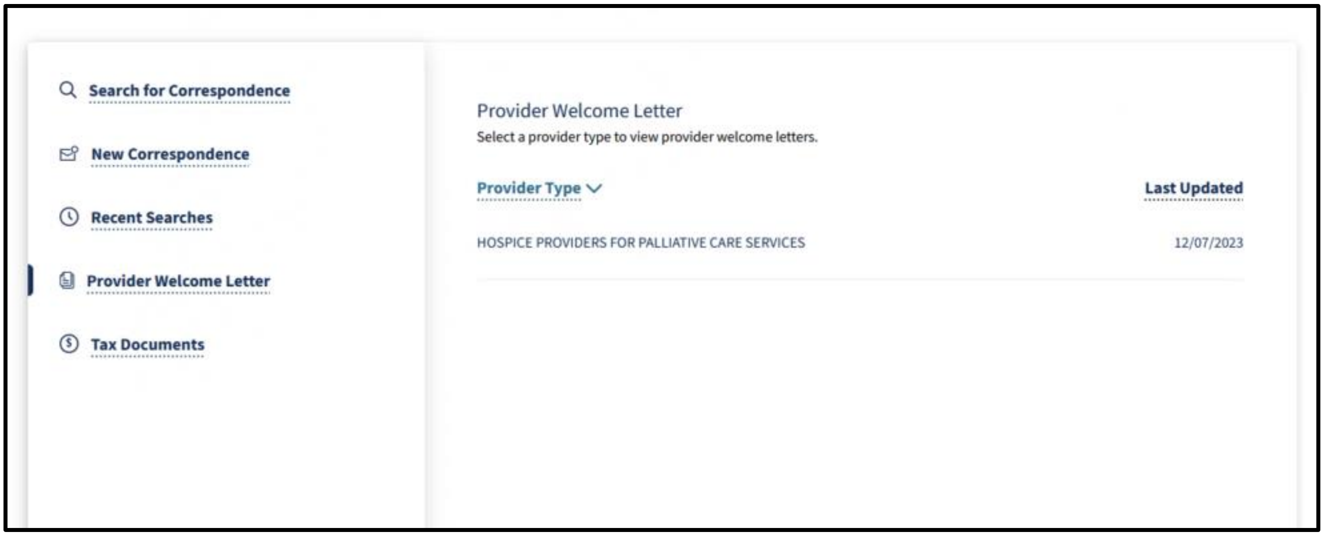


Figure 2.92: Provider Welcome Letter.

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

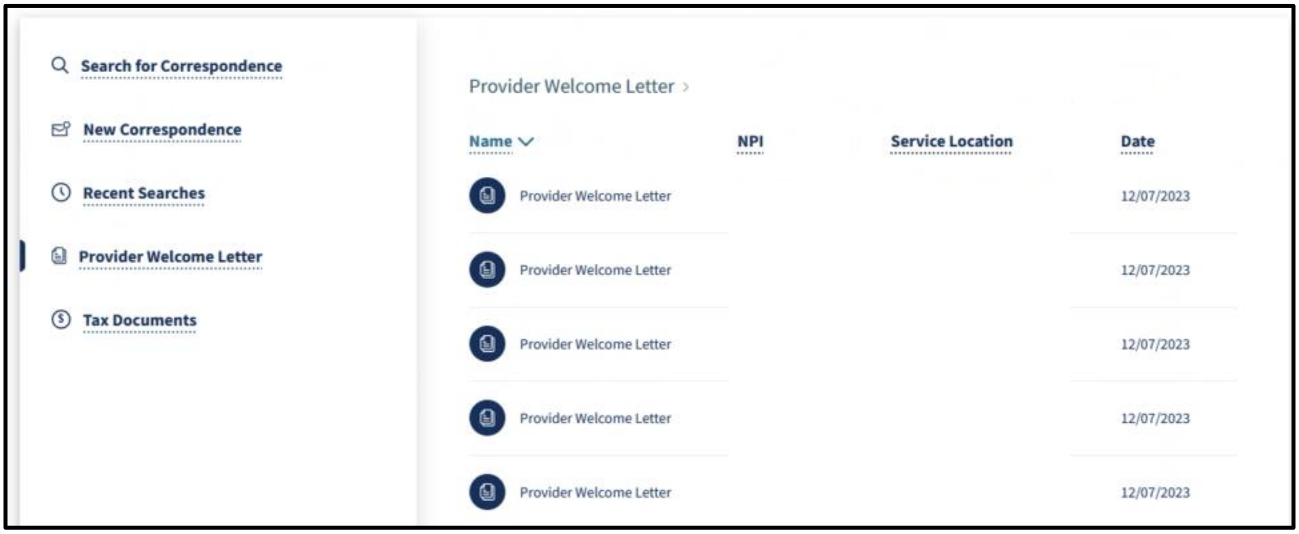
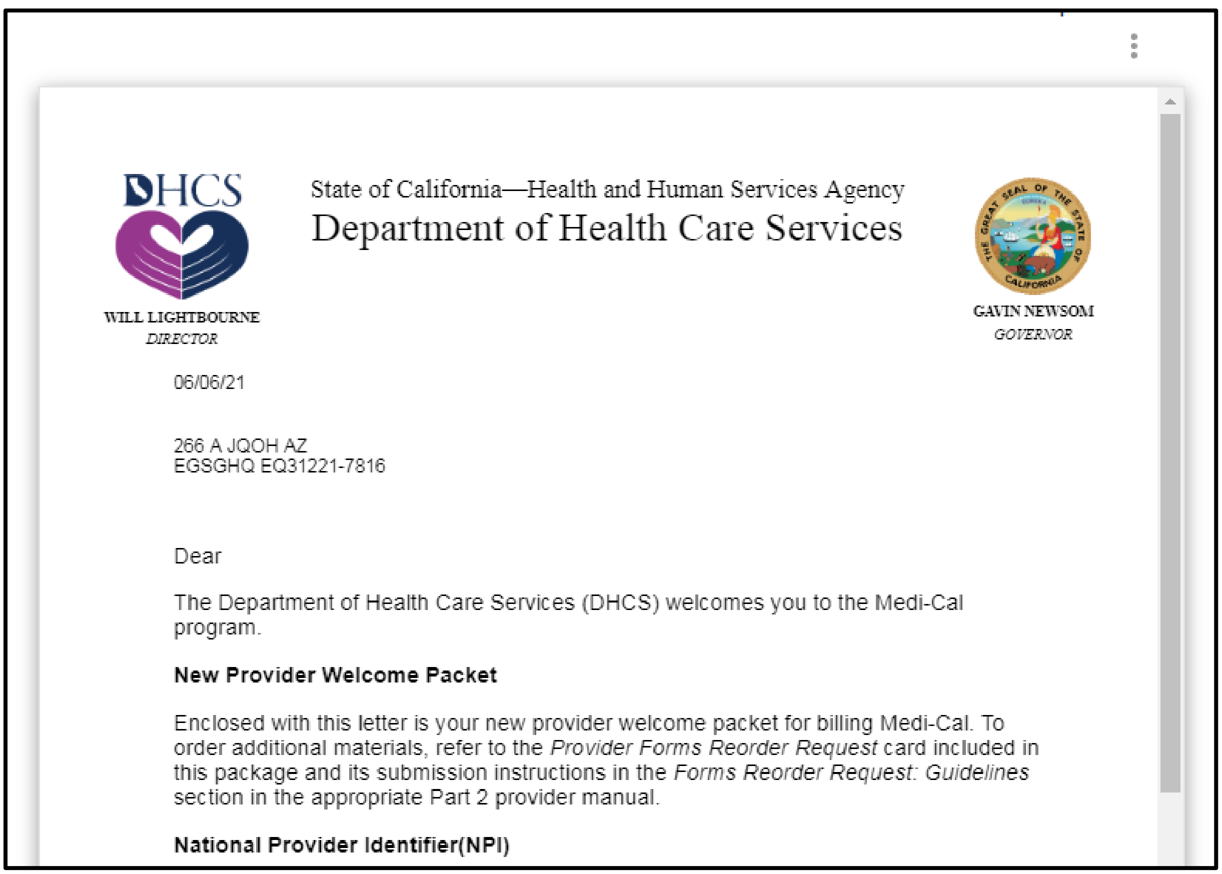


Figure 2.93: List of Provider Welcome Letters.

3. A PDF version of the letter appears.



DHCS

WILL LIGHTBOURNE
DIRECTOR

State of California—Health and Human Services Agency
Department of Health Care Services

GAVIN NEWSOM
GOVERNOR

06/06/21

266 A JQOH AZ
EGSGHQ EQ31221-7816

Dear

The Department of Health Care Services (DHCS) welcomes you to the Medi-Cal program.

New Provider Welcome Packet

Enclosed with this letter is your new provider welcome packet for billing Medi-Cal. To order additional materials, refer to the *Provider Forms Reorder Request* card included in this package and its submission instructions in the *Forms Reorder Request: Guidelines* section in the appropriate Part 2 provider manual.

National Provider Identifier(NPI)

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.