State of California
Department of Health Care Services

Medi-Cal Provider Portal User Guide: Submitter Organization

Department of Health Care Services (DHCS)

CA-MMIS

V 1.3

September 2024

Provider Portal User Guide: Submitter Organization

The purpose of the *Provider Portal User Guide: Submitter Organization* is to provide Medi-Cal Submitters with comprehensive instructional documentation on their roles and abilities in the Provider Portal. 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 of the Medi-Cal Providers website that houses personal 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 enables 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 Claim 837 and Eligibility Benefit 270/271 test transactions

How to Register as an Existing Submitter

When registering as an existing submitter, 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 the token has been received, the steps below should be followed:
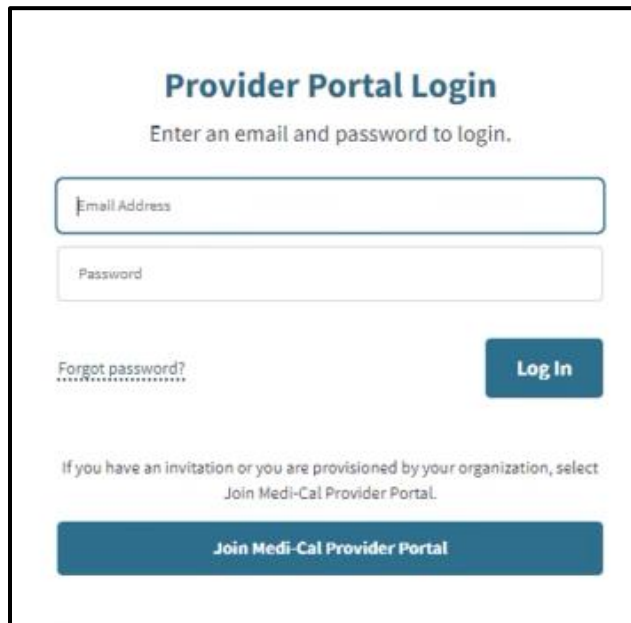
1. Select **Join Medi-Cal Provider Portal**

Figure 1.1: Provider Portal Login.

2. A **Choose Your Organization Type** screen will appear. Select **Submitter Organization**.
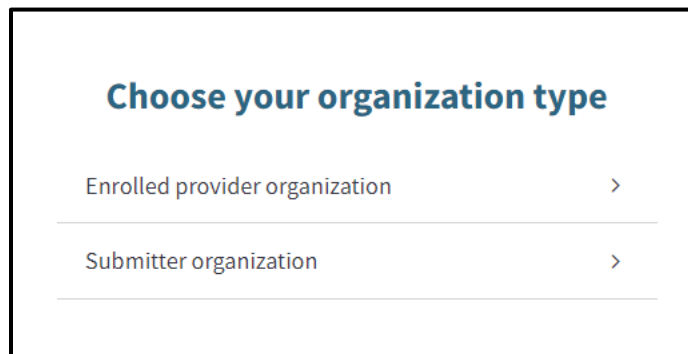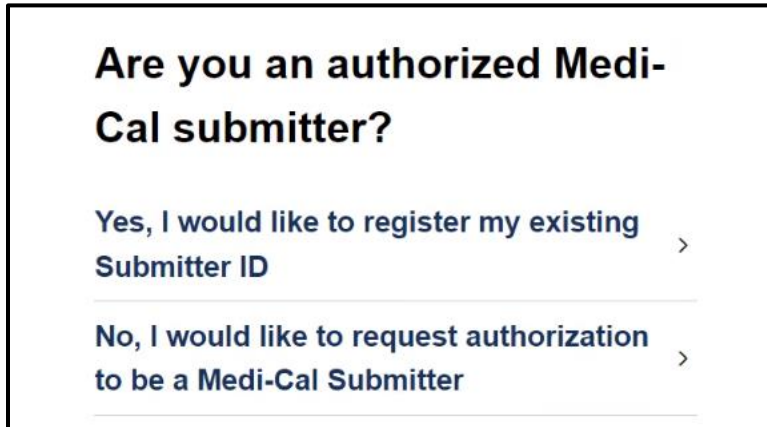
Figure 1.2: Choose your organization type.
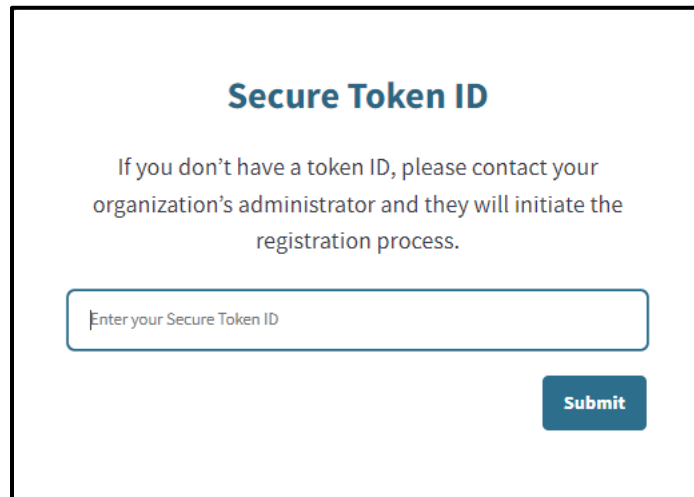
3. A submitter authorization window will appear. Select **Yes, I would like to register my existing Submitter ID**.

Figure 1.3: Medi-Cal Submitter Authorization.

4. Enter the **Secure Token ID** sent from DHCS and then select **Submit**. For a token ID, contact your organization's administrator and they will initiate the registration process.

Figure 1.4: Secure Token ID.

5. Read the terms and conditions, 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 on behalf of my organization**. Once complete, click **Next**.

Figure 1.5: Terms and Conditions for Medi-Cal Provider Portal.

6. Enter in **Submitter Organization Information** (CMC Submitter ID, Business Address ZIP code and the provider's NPI), and **Account Information** (email, first name and last name). Select SMS or Voice to receive passcode, then click **Next**.

Figure 1.6: Organization Information.

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

Note: Depending on the user's phone carrier, there may be a delay in receiving a One-Time Passcode (OTP). Please wait for the OTP to be received. If ten minutes has passed and the user has not received an OTP, the user may click **Resend one-time password**.

Figure 1.7: One-Time Passcode.

8. A **Registration Complete** screen will appear.

Figure 1.8: Registration Complete.

9. Once registration is complete, an email will be sent to set new password for the Provider Portal. The submitter must select the link in the email **within 30 minutes or it will expire.**
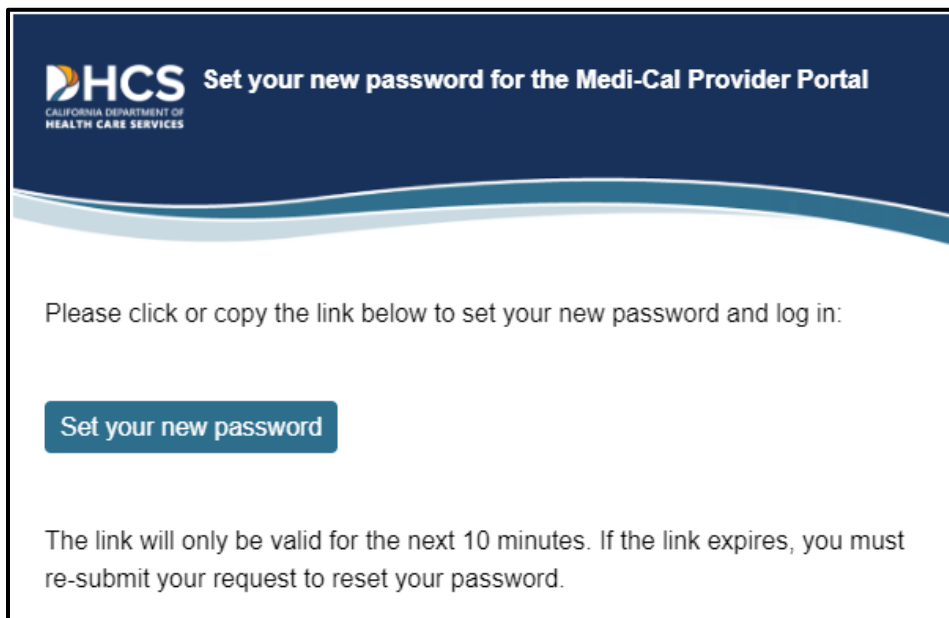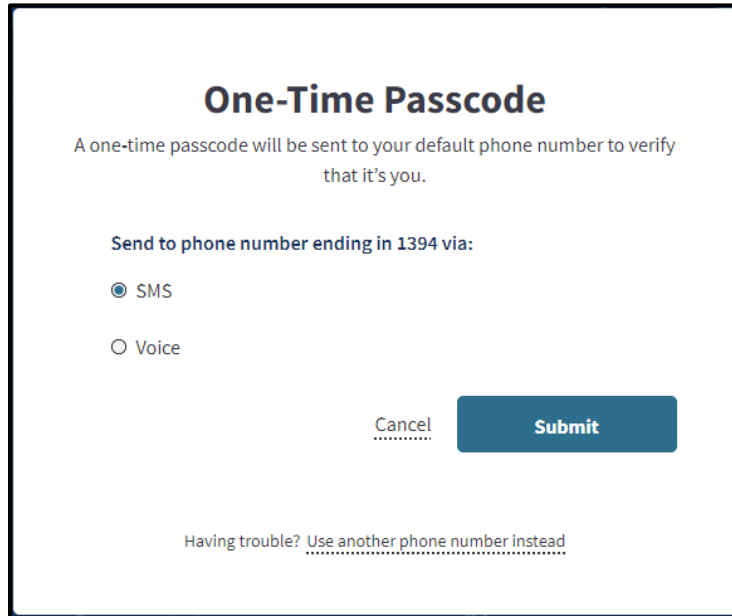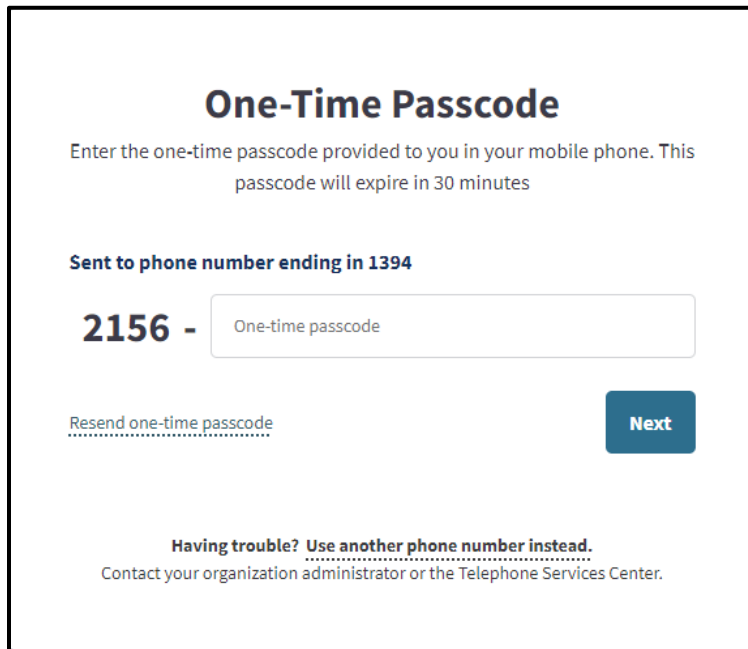

Figure 1.9: Set Your New Password Email Notification.

10. A screen to receive an OTP will appear. Select to receive the passcode via **short message service (SMS)** (text) or by **Voice** (call).

Figure 1.10: One-Time Passcode.

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

Figure 1.11: One-Time Passcode.

12. A screen to **Create New Medi-Cal Password** will appear. Enter a password that aligns with the password criteria and select **Submit**.

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

Figure 1.12: Create New Medi-Cal Password.

13. Once complete, a screen will appear indicating the new password has been successfully updated.
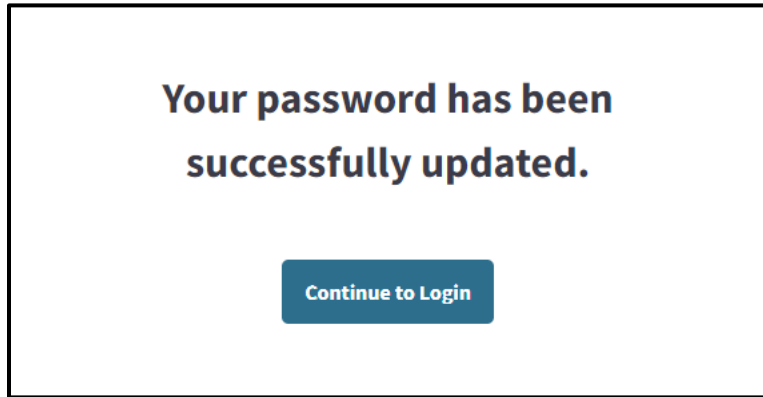
Figure 1.13: Password successfully updated.

14. After completing the registration process, existing submitters will login with the new password.
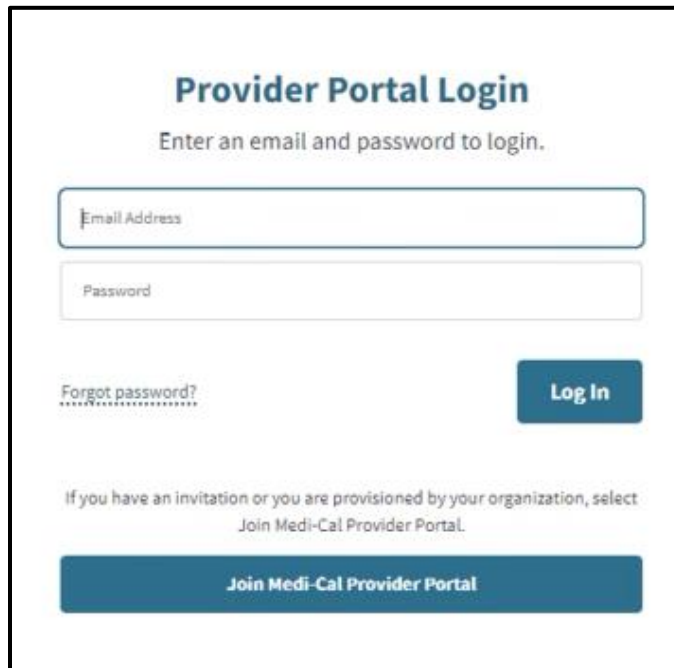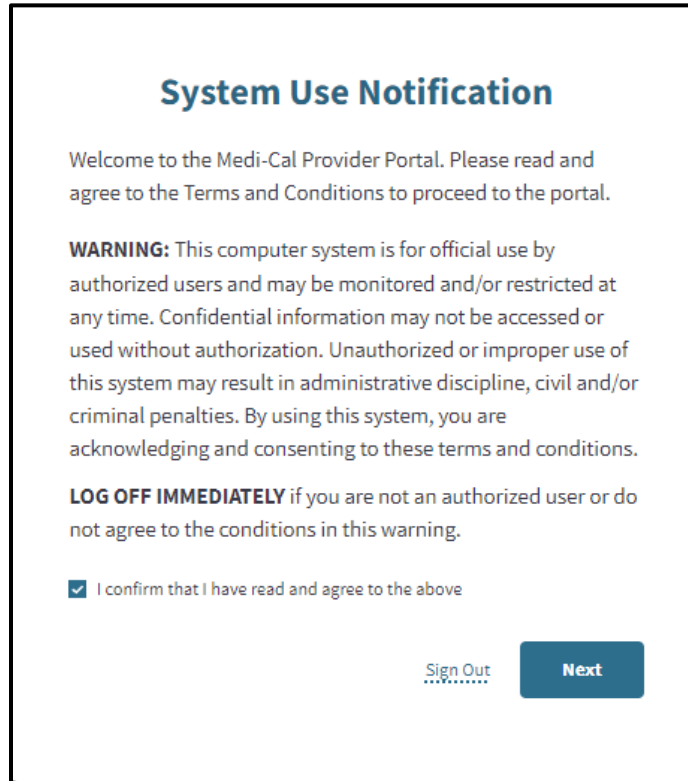

Figure 1.14: Provider Portal Login.

15. A **System Use Notification** screen will appear. Select **I confirm that I have read and agree to the above** and click **Next**.

Figure 1.15: System Use Notification.

Register as a New Submitter

1. Click **Join Medi-Cal Provider Portal**.
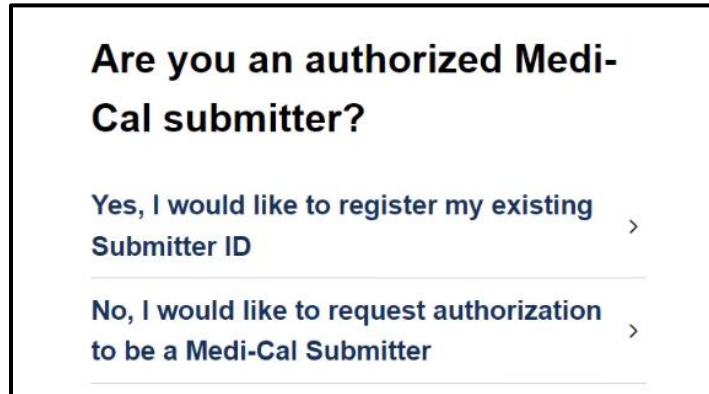

Figure 1.16: Provider Portal Login.

2. A **Choose Your Organization Type** screen will appear. Click **Submitter Organization**.
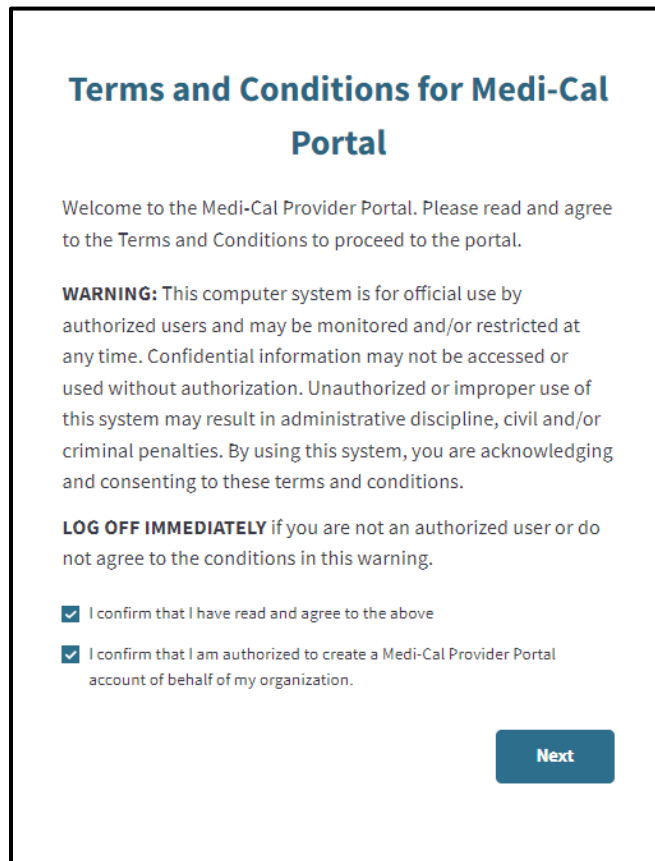

Figure 1.17: Choose your organization type.

3. A submitter authorization window will appear. Click **No, I would like to request authorization to be a Medi-Cal Submitter**.

Are you an authorized Medi-Cal submitter?

Yes, I would like to register my existing Submitter ID   >

No, I would like to request authorization to be a Medi-Cal Submitter   >

Figure 1.18: Medi-Cal Submitter Authorization.

4. Read the terms and conditions, 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 on behalf of my organization**. Once complete, click **Next**.

Terms and Conditions for Medi-Cal Portal

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

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

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

☑ I confirm that I have read and agree to the above

☑ I confirm that I am authorized to create a Medi-Cal Provider Portal account of behalf of my organization.

Next

Figure 1.19: Terms and Conditions for Medi-Cal Portal.

5. An **Organization Information** screen will appear. Enter the **Submitter Organization Information**, **Affiliated Provider Organization** and **Account Information.** Select SMS or Voice to receive passcode, then click **Next**.

Organization Information

Enter the following information to begin the process to enroll with Medi-Cal as a new Biller/Submitter organization.

STOP: If you are already an approved Biller/Submitter you will want to register your existing account with Medi-Cal.

Submitter Organization Information

Submitter Legal Name

Doing Business As Name (DBA) - if applicable

Organization Phone Number

Address Line 1

Address Line 2 (optional)

City

State: CA — Zip

Affiliated Provider Organization

You must affiliate with a provider organization to gain full access to the Provider Portal. Please enter the provider tax ID and one billing NPI in the organization that is actively enrolled. Please note: entering an NPI is for verification purposes only. The organization admin will assign access to NPIs after approval.

Enter an affiliated provider organization to verify your registration.

Provider EIN/SSN

NPI

Account Information

Email Address

First Name

Last Name

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

Preferred Contact Number

Receive passcode via:
◉ SMS
◯ Voice
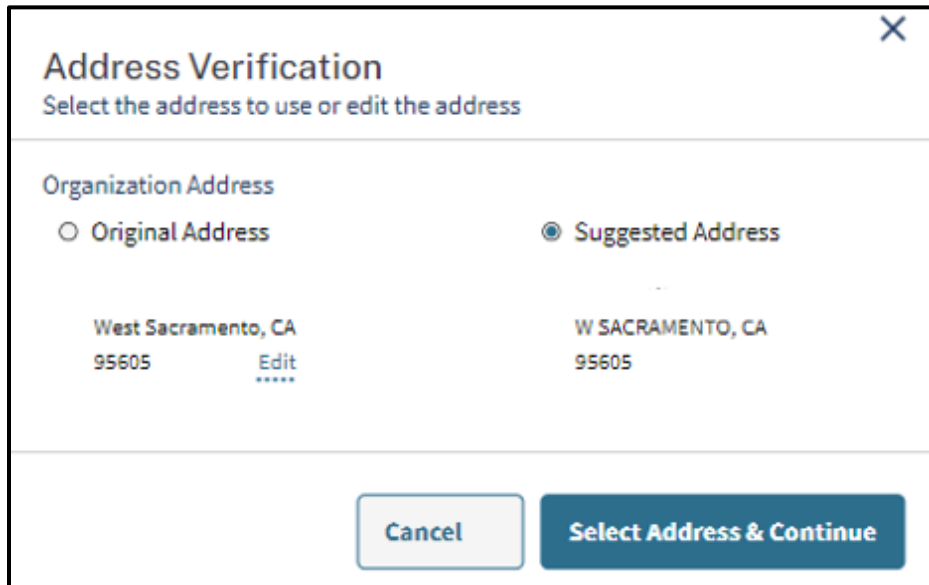
Next

Figure 1.20: Organization Information.

6. An **Address Verification** screen appears. Select the correct address and click **Select Address & Continue**.

Figure 1.21: Address Verification.

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

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

One-Time Passcode

Enter the one-time passcode provided to you in your mobile phone. This passcode will expire in 30 minutes

Sent to phone number ending in 1394

9567 - [One-time passcode]

Resend one-time passcode   Next

Having trouble? Use another phone number instead.
Contact your organization administrator or the Telephone Services Center.

Figure 1.22: One-Time Passcode.

8. A screen for **Medi-Cal Online Conditions of Use Agreement** will appear. Select **I am authorized to attest and agree to all the terms and conditions of this agreement on behalf of my organization,** and **I have read and agree to these conditions of use on behalf of my organization**. Once complete, select **Next**.

Figure 1.23: Medi-Cal Online Conditions of Use Agreement.

9. A screen for the *Medi-Cal Telecommunications Provider and Biller Application/Agreement* (DHCS 6153) form will appear. Please read the agreement form and then sign with First and Last name along with Title. Once complete, select **Submit Agreement**.

Figure 1.24: Medi-Cal Telecommunications Provider and Biller Application/Agreement.

10. **Registration Complete** screen for affiliation request will appear.
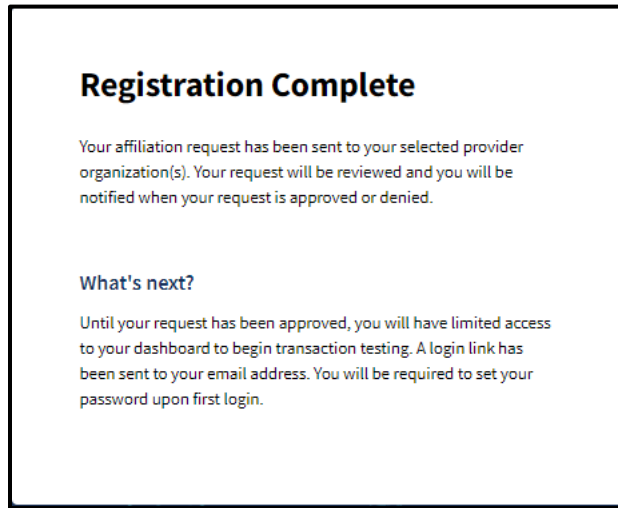
Figure 1.25: Registration Complete.

11. Once registration is complete, an email will be sent to set new password for the Provider Portal. The submitter must select the link in the email **within 30 minutes or it will expire.**
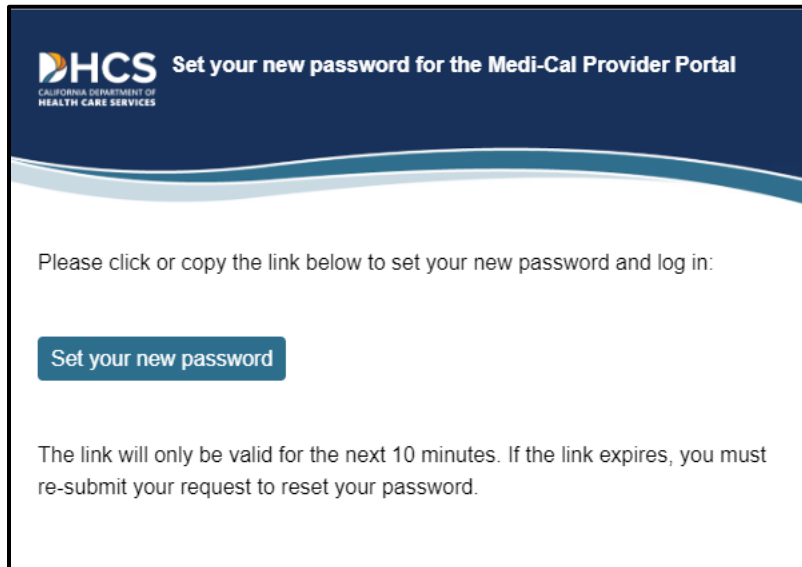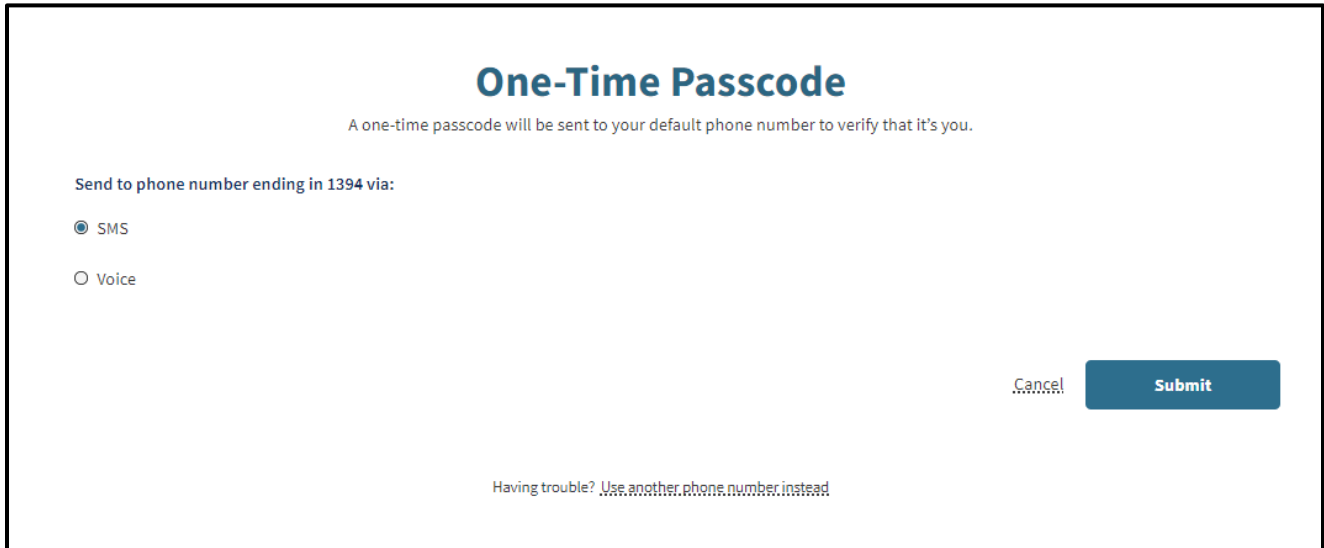

Figure 1.26: Set Your New Password Email Notification.
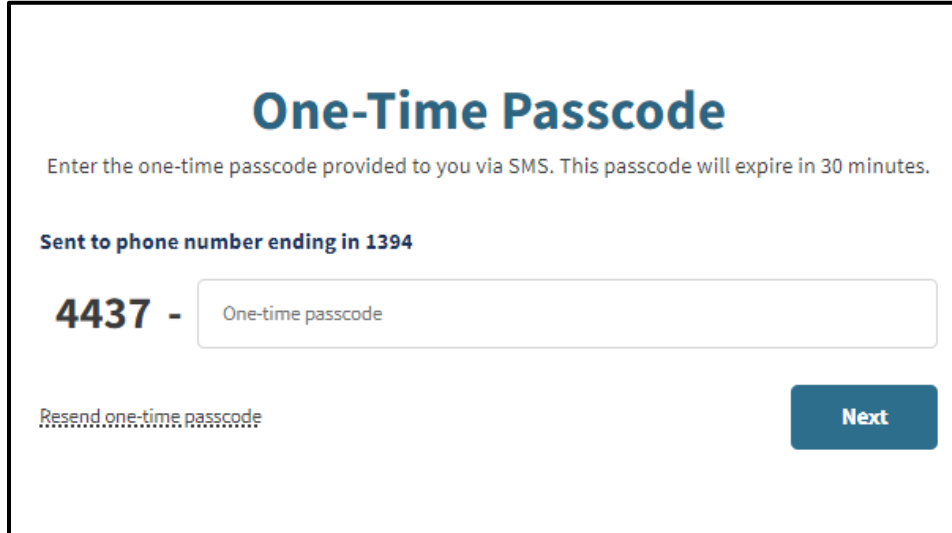
12. A screen to receive an OTP will appear. Select to receive the passcode via **SMS** or **Voice**.

Figure 1.27: One-Time Passcode.

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

Figure 1.28: One-Time Passcode.

14. A screen to **Create New Medi-Cal Password** will appear. Enter a password that aligns with the password criteria and click **Submit**.
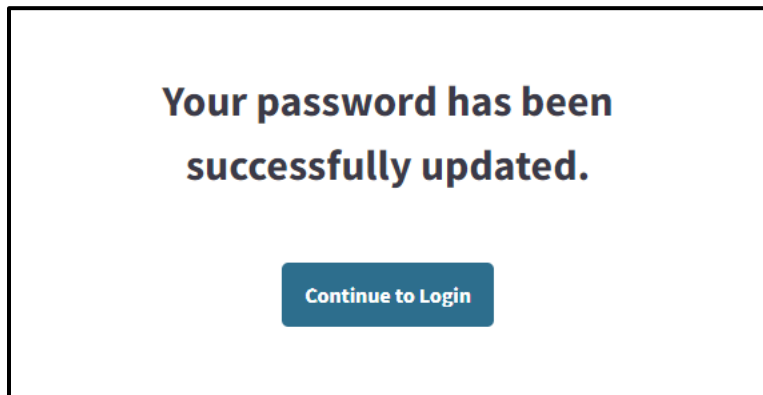
Note: The password must be a minimum of 15 characters and must include at least one uppercase letter, one lowercase letter, one numeral and one special character. A recently used password cannot be reused.

Figure 1.29: Create New Medi-Cal Password.

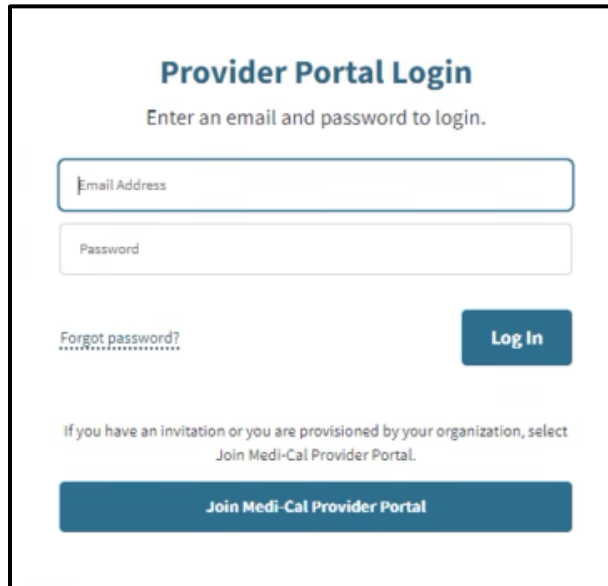15. Once complete, a screen will appear indicating the new password has been successfully updated.

Figure 1.30: Password successfully updated.
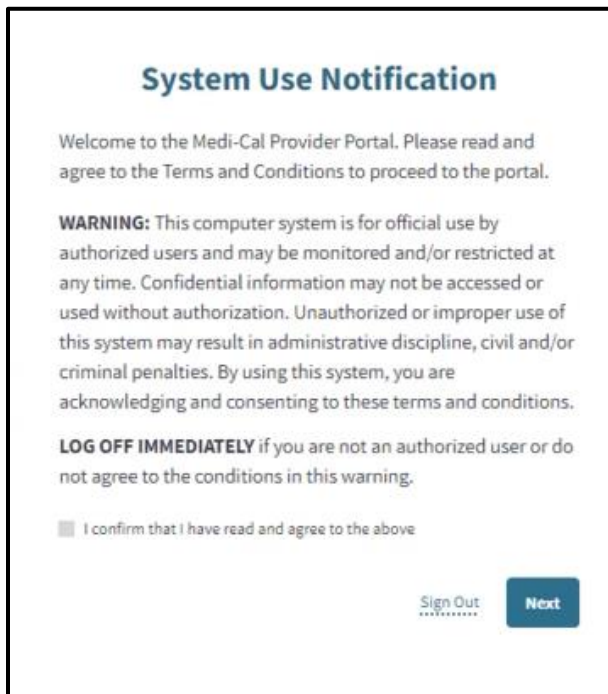
16. After completing the registration process, existing submitters will login with the new password.

Figure 1.31: Provider Portal Login.

17. A **System Use Notification** window displays. Select **I confirm that I have read and agree to the above** and click **Next**.
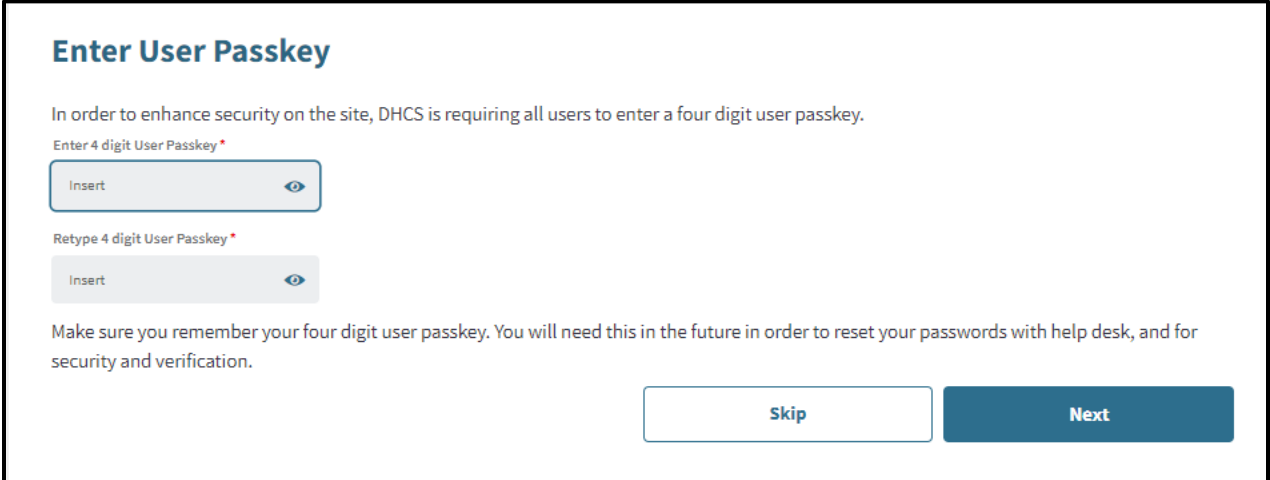

Figure 1.32: System Use Notification.

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 1.33: Enter User Passkey.

Provider Portal Overview

The Provider Portal is designed to house communications, notifications and organization information. Users within a submitter organization may 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 submitter features within the Provider Portal such as Transaction Testing and access to Transaction Center but will not have access to the organization administration functions.
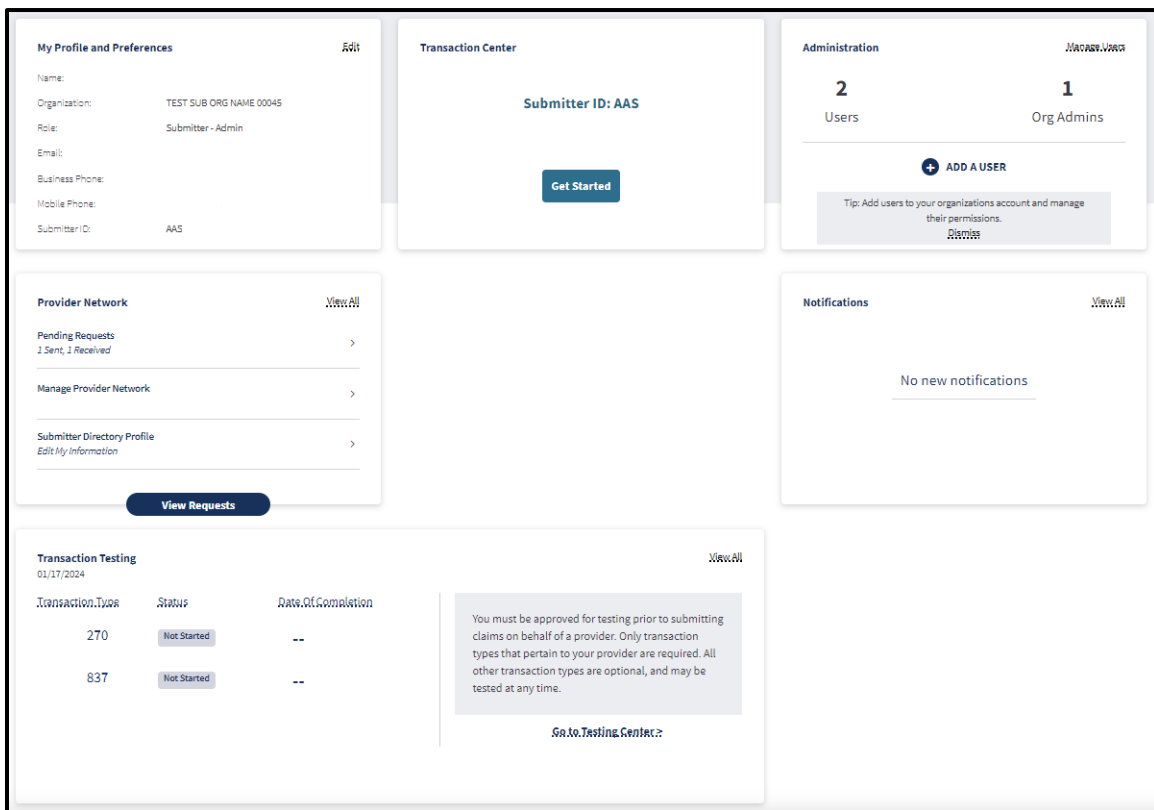
Dashboard

Figure 1.34: Provider Portal Submitter Admin Dashboard.

The Portal contains six (6) areas on an Administrator's Dashboard; detailed information about each can be found later in this user guide.

- **My Profile and Preferences** contains personal contact information and submitter ID. This allows adjustment to email notification settings.

- The **Transactions Center** allows users to create and keep track of various transactions, and single sign on to Transaction Services.

- **Administration** displays information about users within an organization. This area permits Administrators to update user permissions and information, and add and/or remove user profiles.

- **Provider Network** area allows a user to electronically search, view and download correspondence related to the organization. A user may search by NPI, document type or date.

- **Notifications** allows a user to view unread and past notifications about an organization. Notifications can be searched for or filtered by date.

- **Transaction Testing** allows a user to submit transaction testing for 837 and 270 claim transactions.

Account Status Bar

The **Account Status** bar located on the bottom of the Dashboard page displays the approval status of: **Submit affiliation request(s)**, **Complete transaction testing** and **Receive provider approval**. The bar will read **Pending approval** until all three tasks are checked. Once they are all complete, the bar will disappear.
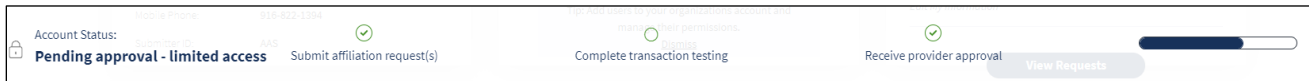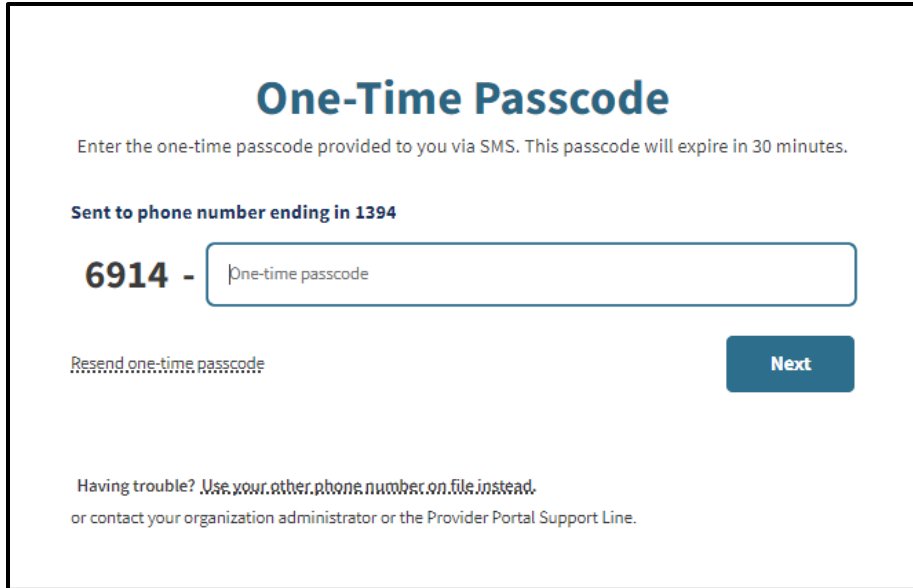

Figure 1.35: Account Status Dashboard.

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 1.36: One-Time Passcode.

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

To edit phone settings, refer to the "Edit Phone Number" section in this user guide.

Select an Organization

Upon first login, a screen appears prompting the new user to select an organization. The organizations displayed are determined by an Administrator when the Administrator is 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.
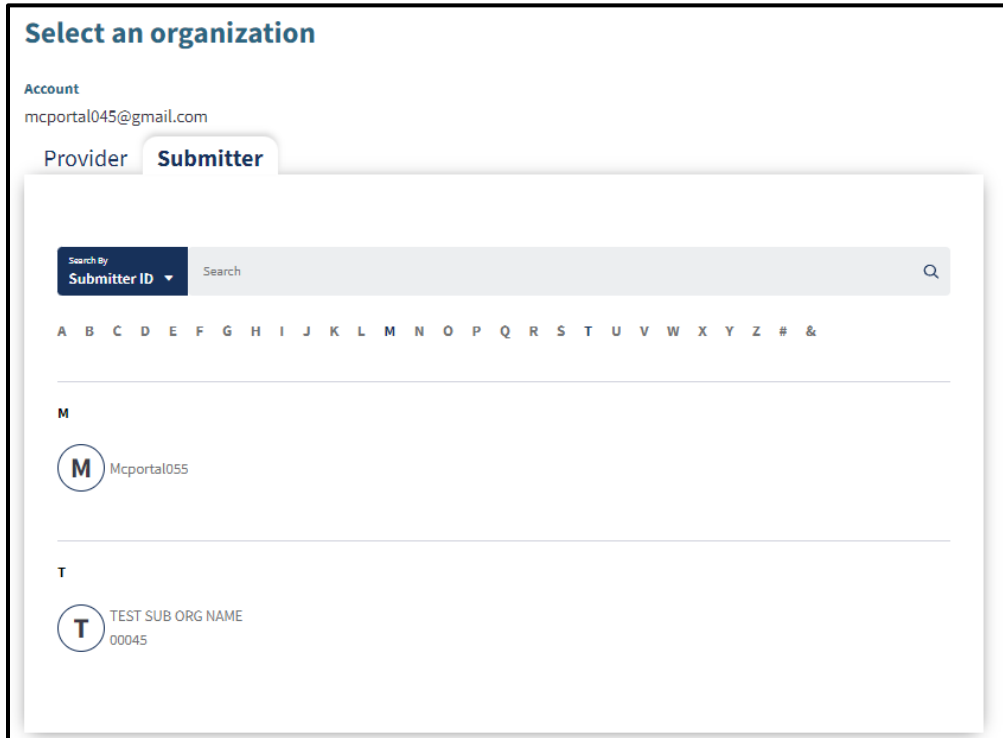
Figure 1.37: Select an organization.

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

Switch to a Different Organization

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 top right-hand side of the **Dashboard**, then selecting **Switch Organization**.
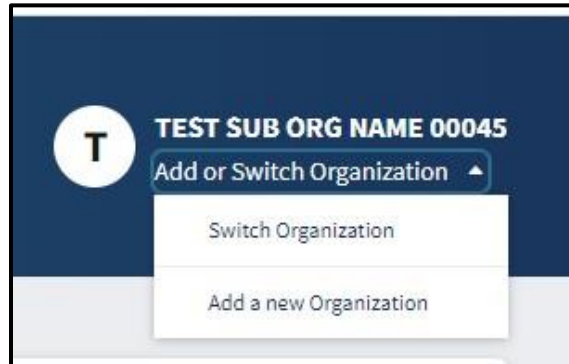
Figure 1.38: Add or Switch Organization.

2. The **Select an Organization** page appears and the user can switch organizations by selecting one of the items on the list.
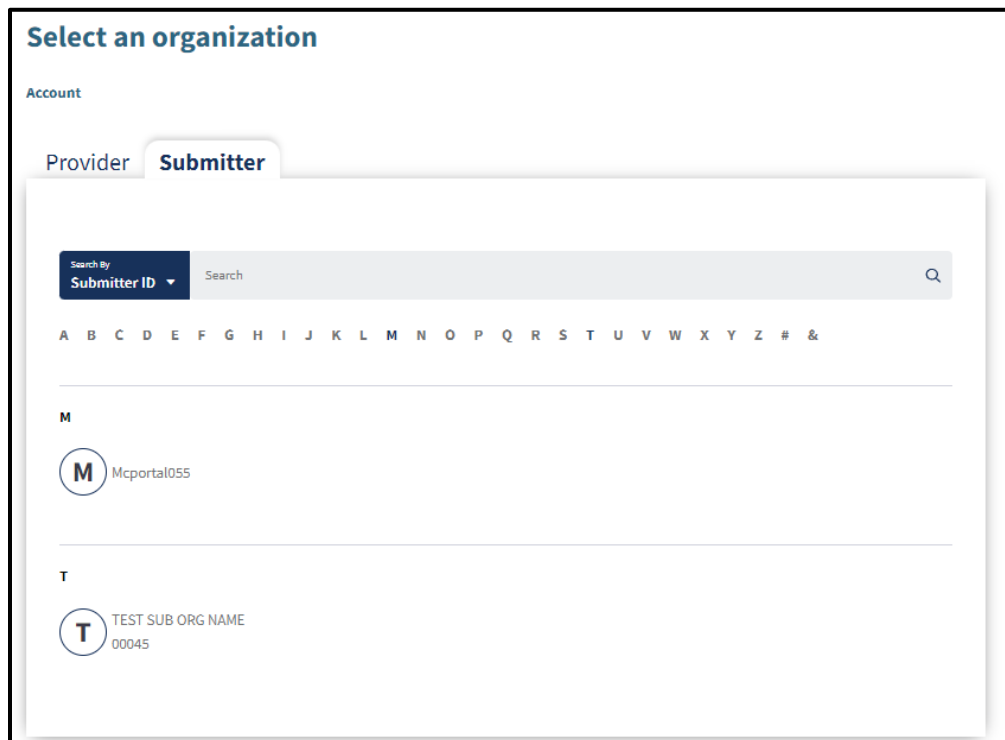
Figure 1.39: Select an organization.

Add New Organization

1. If a user wishes to add a new organization, the user can do so at any time by clicking the **Add or Switch Organization** drop-down menu from the top right-hand side of the **Dashboard**, then selecting **Add a new organization**.
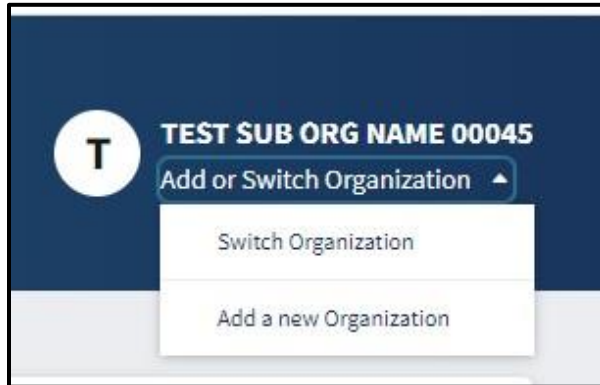
Figure 1.40: Add or Switch Organization.

Change a Password

Users may change their own passwords:

1. From **My Profile and Preferences** on the **Dashboard**, select **Edit**.
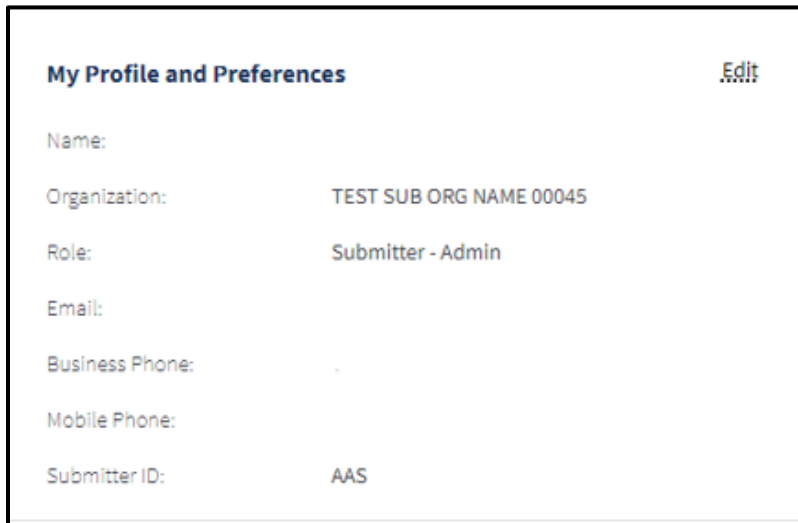
Figure 1.41: My Profile and Preferences.

2. A page to **Edit Account Information** appears. Scroll down to Password and click **Edit.** An area to edit the account password appears.
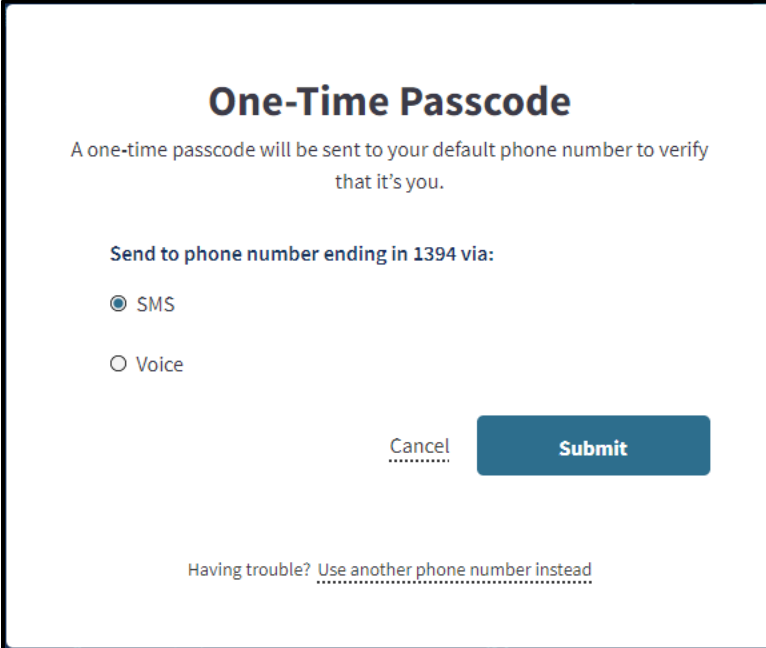
Figure 1.42: Edit Account Information.

3. A screen to receive an OTP will appear. Select to receive the passcode via **SMS** (text) or **Voice** (call).
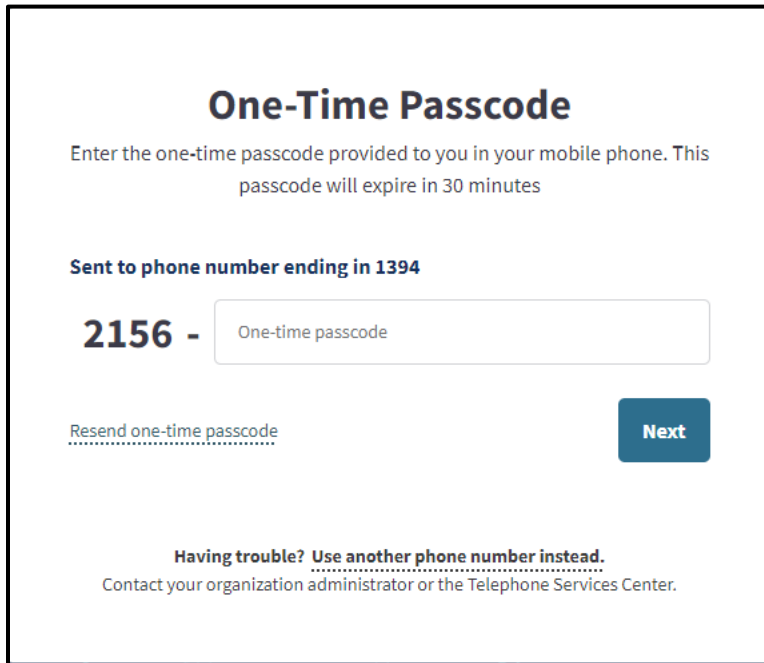
Figure 1.43: One-Time Passcode.

4. Enter the OTP provided. The passcode will expire in 10 minutes.

Figure 1.44: One-Time Passcode.

5. 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.**
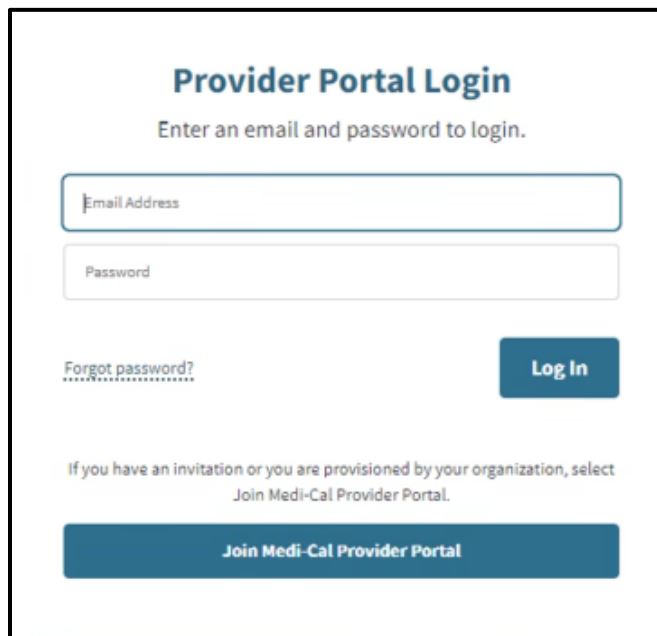
Figure 1.45: Change Password.

6. A confirmation screen appears. The password is now updated.

Reset a Forgotten Password

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

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

Figure 1.46: Provider Portal Login.

2. A **Resend Reset Password Link** screen will appear. Enter the appropriate email address and select **Reset Password**.
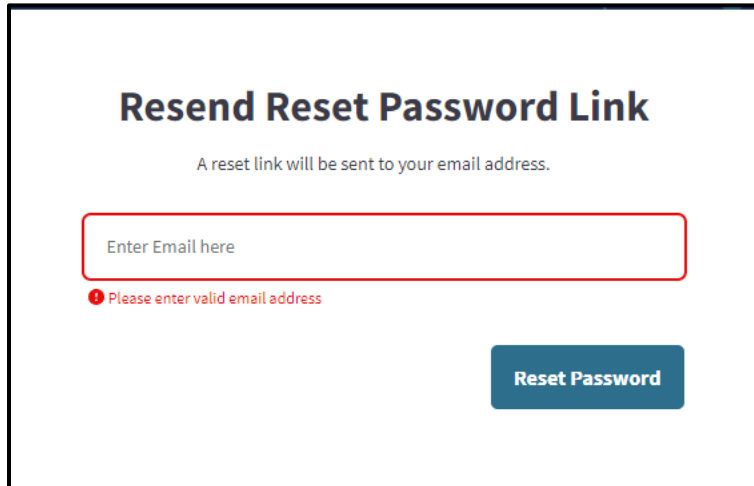
Figure 1.47: Resend Reset Password Link.

3. A notification will appear stating an email has been sent to reset password.
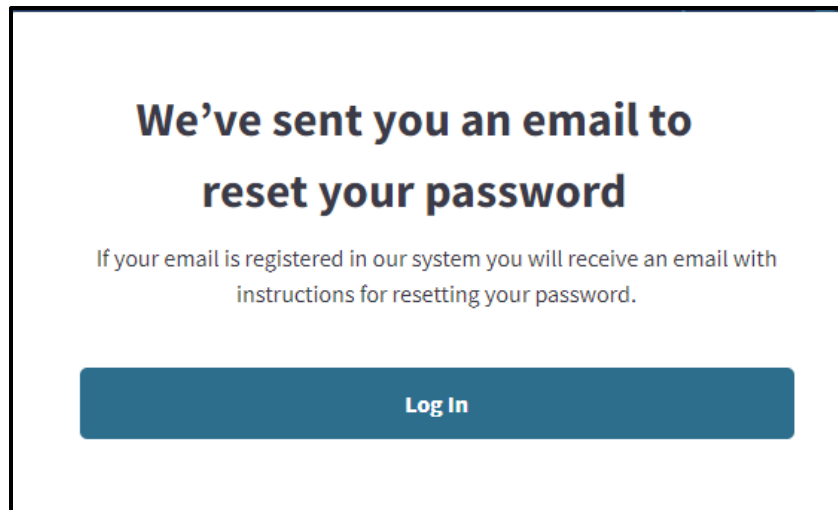
Figure 1.48: Notification of email sent to reset password.

4. A link to reset the password will be sent via email.
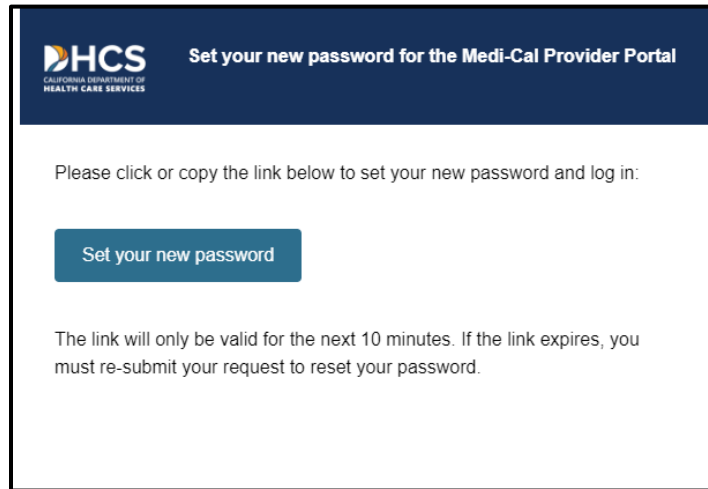
Figure 1.49: Set new password email notification.

5. 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**.
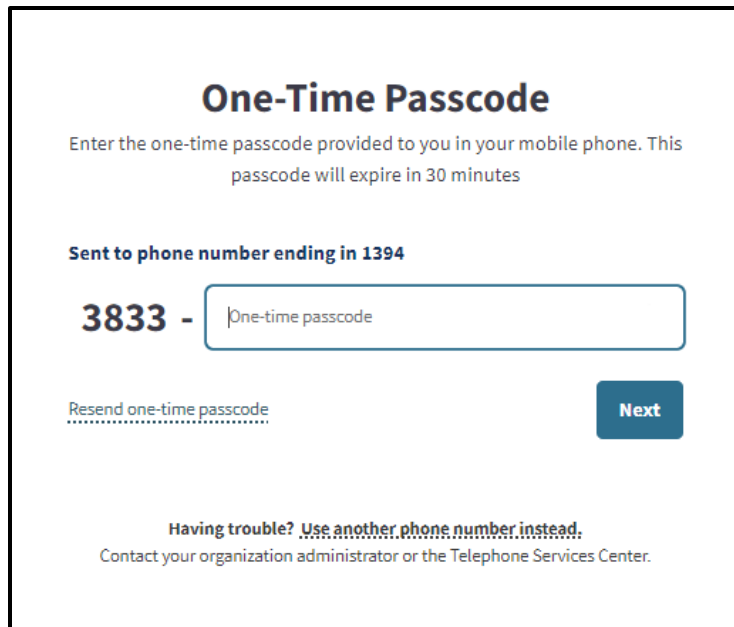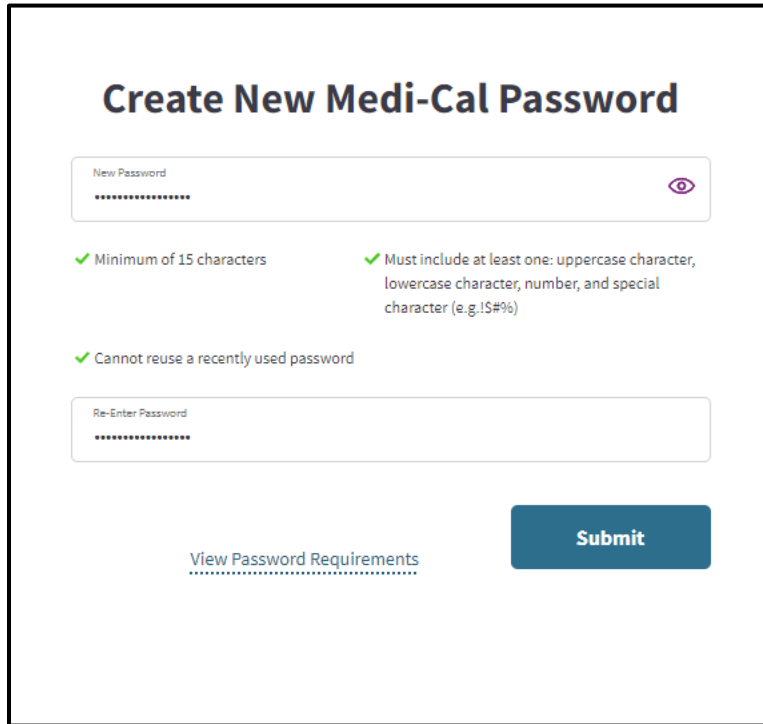
Figure 1.50: One-Time Passcode.

6. 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 1.51: Create New Medi-Cal Password.
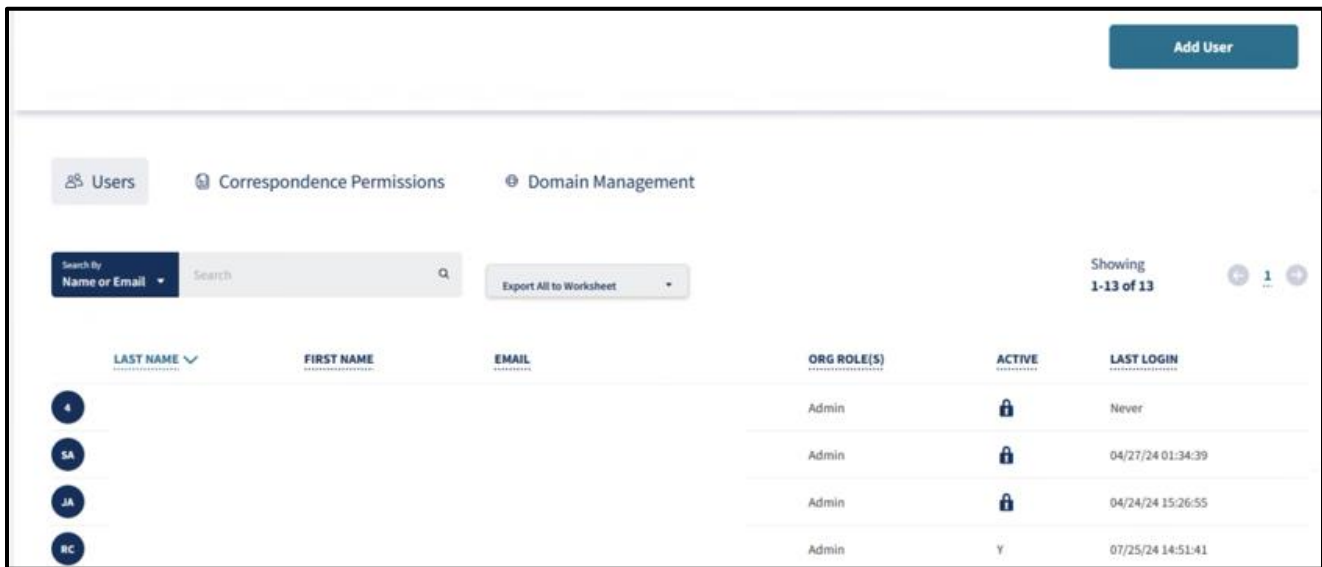
Unlock Account/Reset Password

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 1.52: 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 1.53: Unlock User Account.

3. A pop-up screen will appear. Click **Unlock User Account** to proceed.
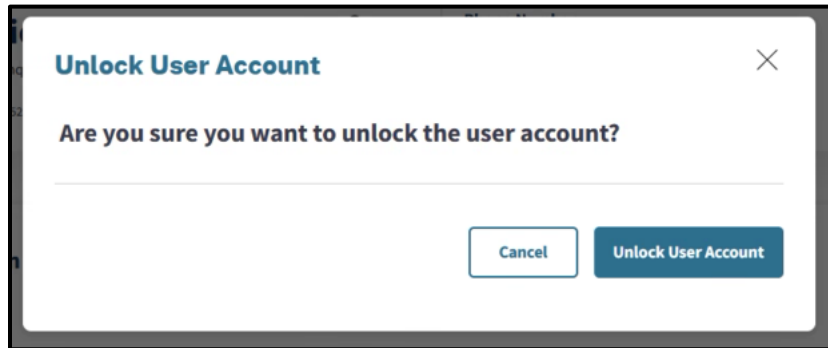
Figure 1.54: Unlock User Account.

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

How to Use Provider Portal Features

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

My Profile and Preferences

The **My Profile and Preferences** area houses personal account information and notification preferences. Personal information can be updated at any time. Follow the steps below:

Edit Personal Information

1. To edit a user's information and preferences, select **Edit** in the **My Profile and Preferences** area on the **Dashboard**:
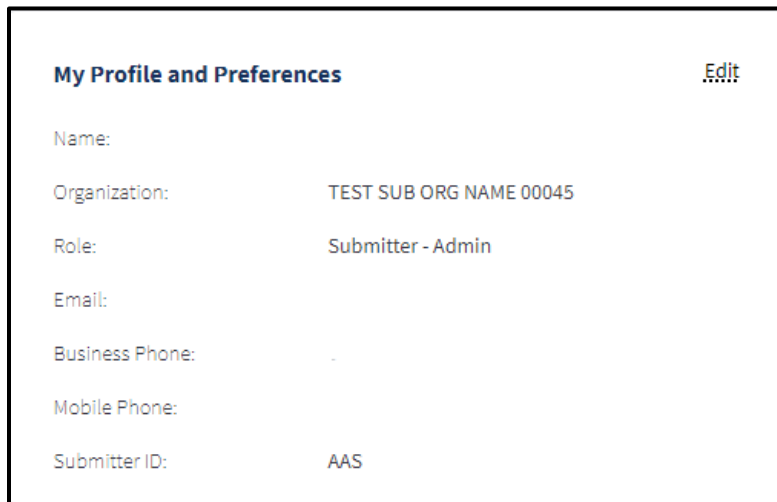
Figure 2.1: My Profile and Preferences.

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

Figure 2.2: Edit Account Information.

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

Figure 2.3: Edit Account 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.

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

Edit Phone Number

1. Select **Edit** next to the phone number to edit.
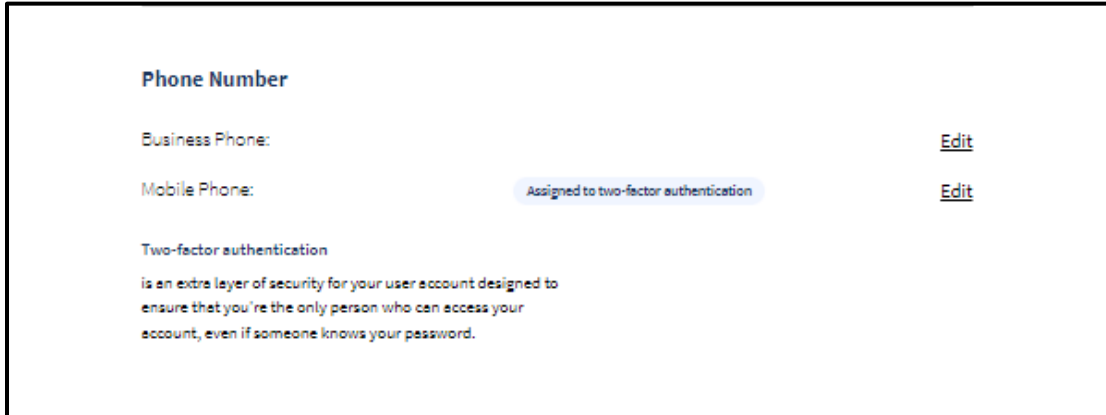
Figure 2.4: Phone Number.

2. 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, select **Use this number for two step authentication**.
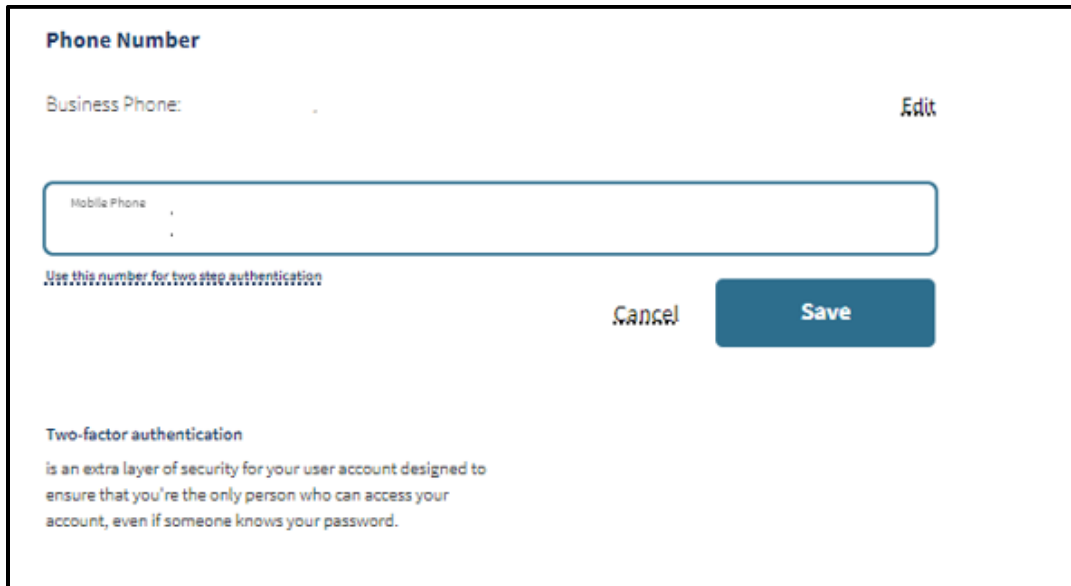
Figure 2.5: Edit Phone Number.

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, a successfully updated user passkey message will appear.
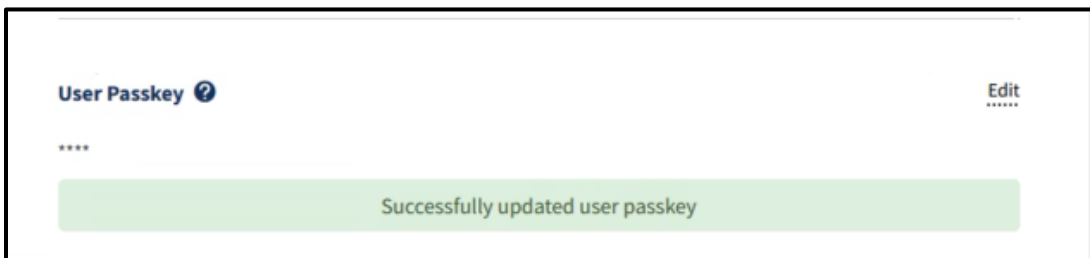
Figure 2.8: Successfully Updated User Passkey.

Edit Notification Preferences

Users automatically receive notifications in the Provider Portal via the **Notifications** area. This setting is automatically selected and cannot be changed. However, if a user would like to receive notifications via email, they can select the **Email** checkbox next to the desired notification.
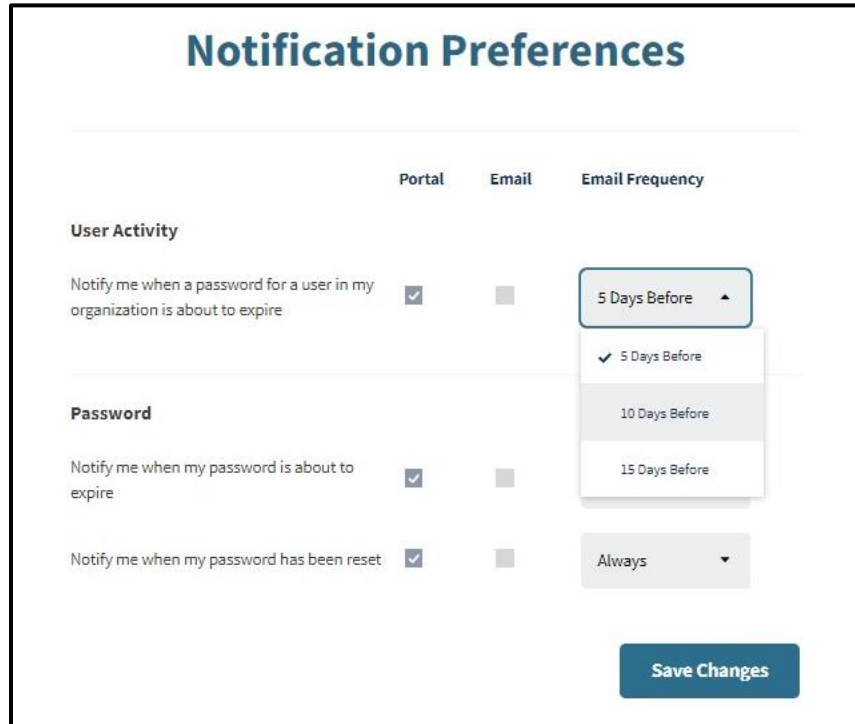
Figure 2.9: Notification Preferences.

Page updated: July 2023
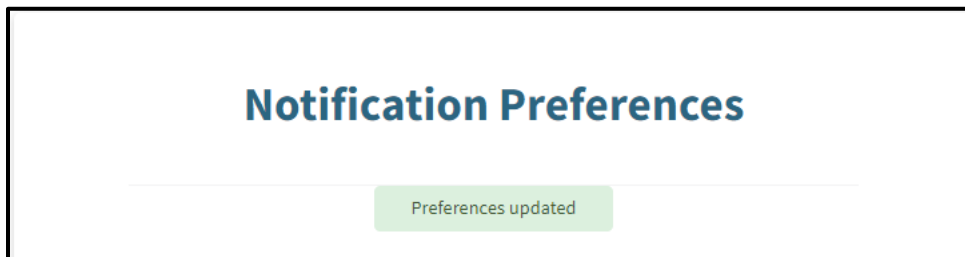
1. To change the frequency of a notification, click the **Notification Frequency** dropdown menu next to the specific notification to update the setting.

Figure 2.10: Notification Frequency.

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

Figure 2.11: Notification Preferences Successfully Edited.

Edit Submitter Directory Information

This area may only be accessed by individuals who are designated as organization admins.

Figure 2.12: Edit Submitter Directory Information.

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

Figure 2.13: Edit Organization Information.

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

Figure 2.14: Edit Personal Information.

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

Figure 2.15: Submitter Information Successfully Updated.
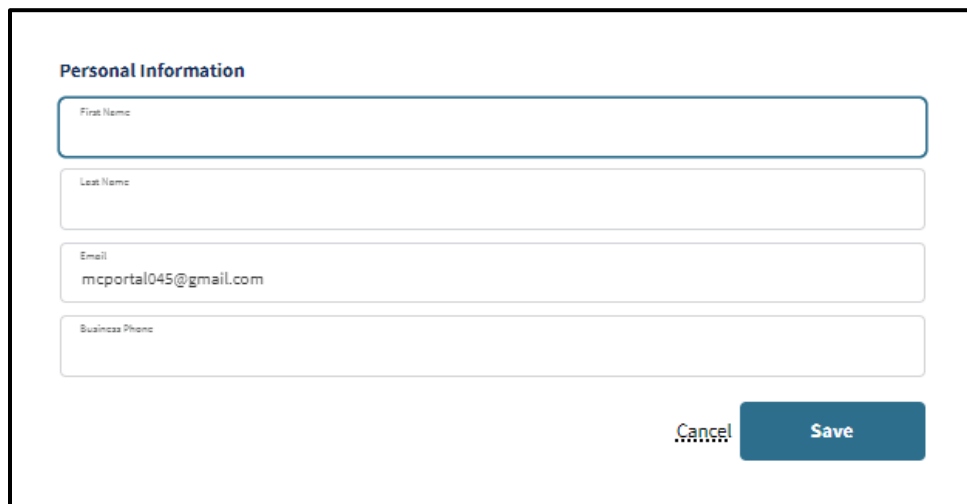
4. Click **Edit** next to Contact Information.

Contact Information   Edit

Name:

Email:

Phone Number:

Figure 2.16: Edit Contact Information.

5. Update the desired information and click **Save**.
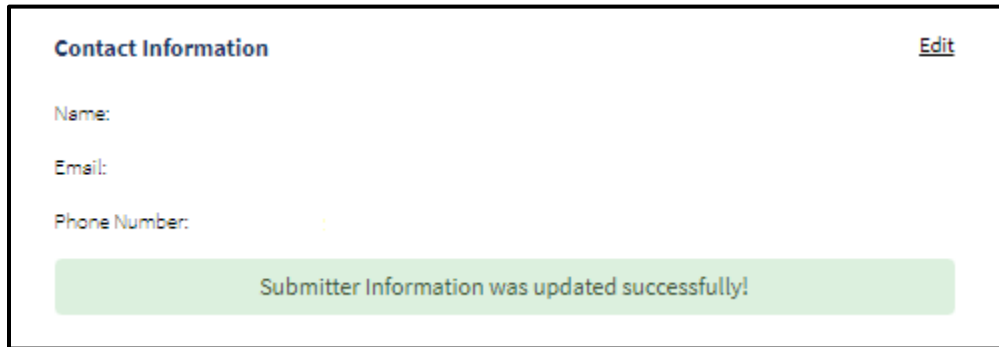
Personal Information

First Name

Last Name

Email

mcportal045@gmail.com

Business Phone

Cancel   **Save**

Figure 2.17: Edit Personal Information.
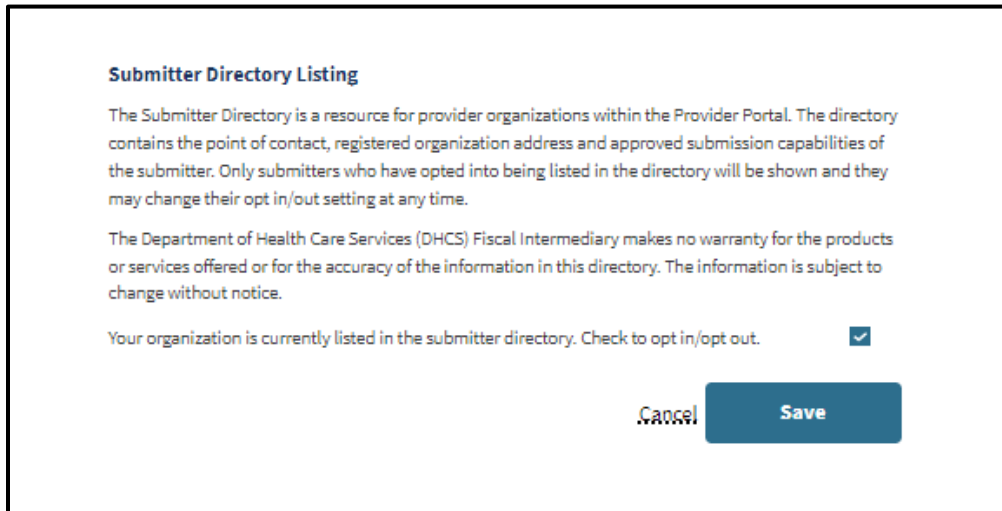
6. A confirmation appears indicating the updated information was successfully updated.

Figure 2.18: Submitter Information Successfully Updated.

7. The Submitter Directory contains the point of contact, registered organization address and approved submission capabilities of the submitter. Only submitters who have opted into being listed in the directory will be shown and they may change their opt in/out setting at any time. Click **Edit** next to Submitter Directory Listing.

Figure 2.19: Submitter Directory Listing.

Note: This area may only be accessed by those who are designated as Administrators of the submitter organization.

Transaction Center

Provider Portal users may access Transaction Services by secure single sign-on. Users may search transactions by clicking the **Get Started** link within the Transaction Center tile on the Provider Portal **Dashboard**.
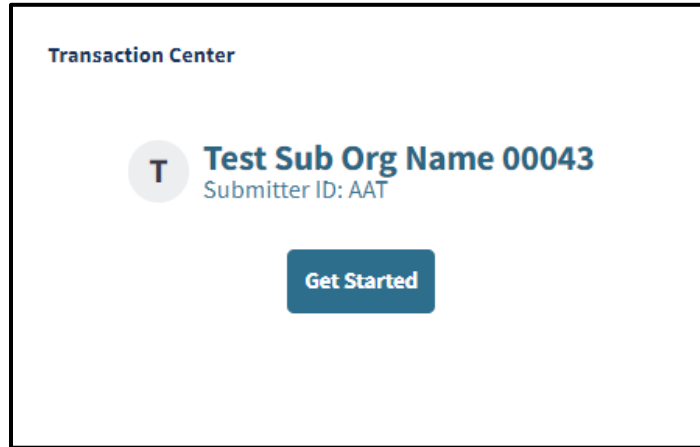

Figure 2.20: Transaction Center Tile.

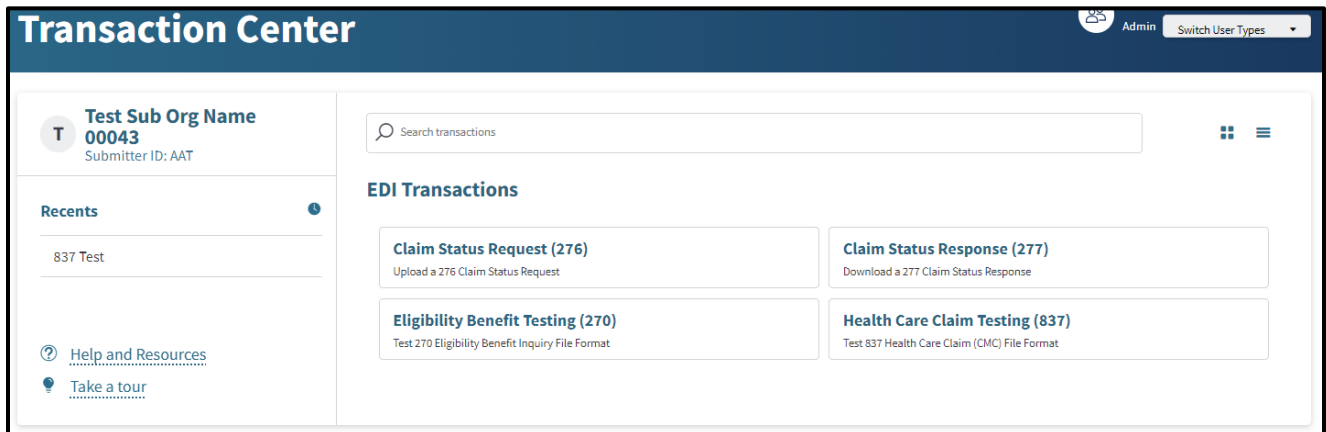From here, the user may search or view the transactions.

Figure 2.21: Transaction Center.

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 admins.

Add User

1. To add a new user to an organization, select **Add A User** or **Manage Users** within the Administration tile.
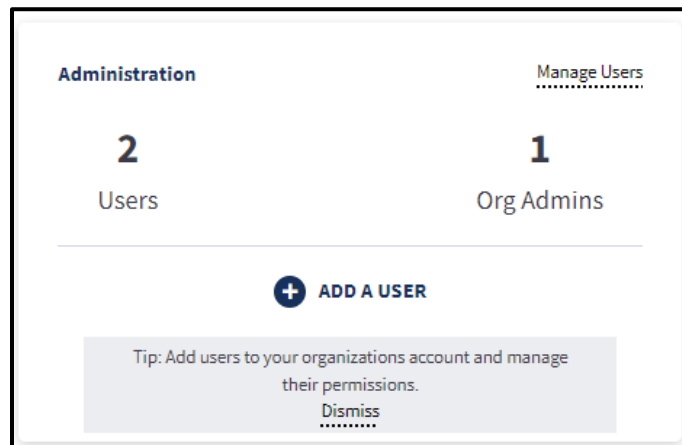

Figure 2.22: Administration Tile.

2. An **Add a User** screen will display. Enter in the **Email Address**, **First and Last Name**, **Mobile Number** and **Business Number** of the added user and select **Next**.
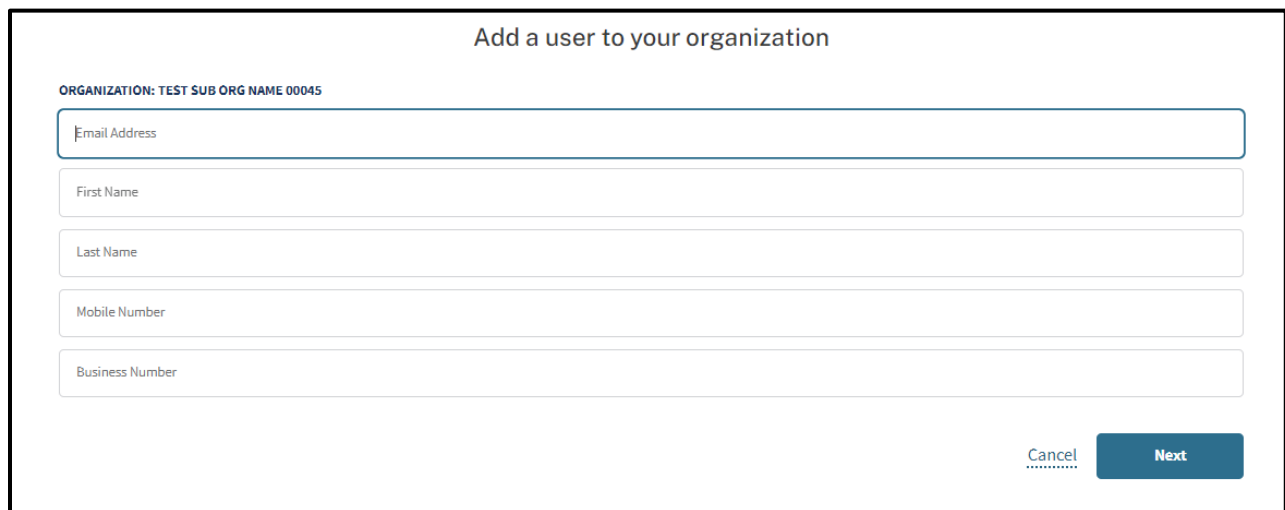
Figure 2.23: Add a User to Your Organization.

3. Once complete, a screen to assign the user's organization role will appear.

Figure 2.24: Assign Role.

4. Select the organization role type by clicking the drop-down menu under **Assign Role** to assign the role of either **Processor** or **Administrator**. Once the role type is selected, click **Save and Finish**.

Figure 2.25: Assign Role.

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

5. Once complete, the **User Management and Permissions** screen will appear, the new user will be added and they will receive an email to complete their registration.
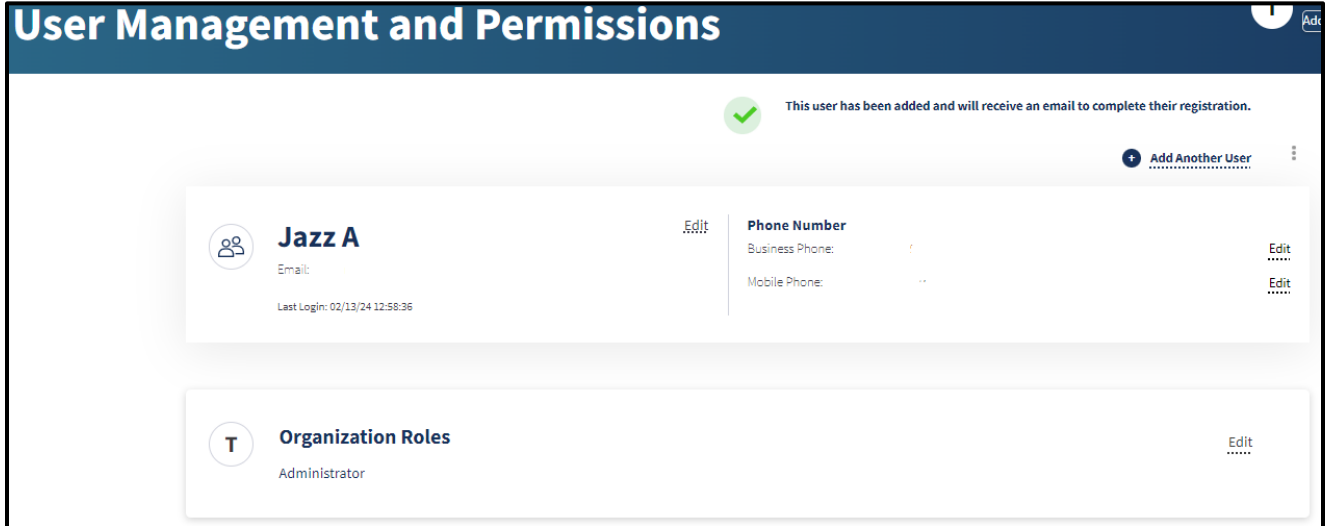
Figure 2.26: User Management and Permissions.

6. The new user and their organization role will be listed under Users.
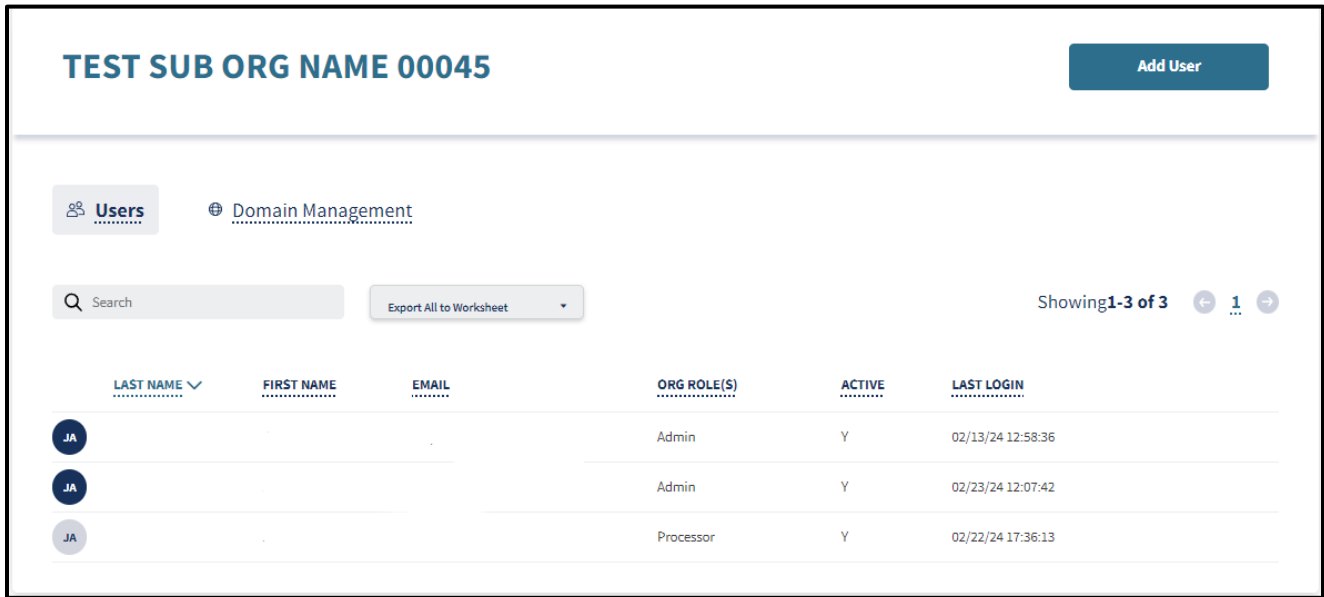
Figure 2.27: Manage Users.

Deactivate User

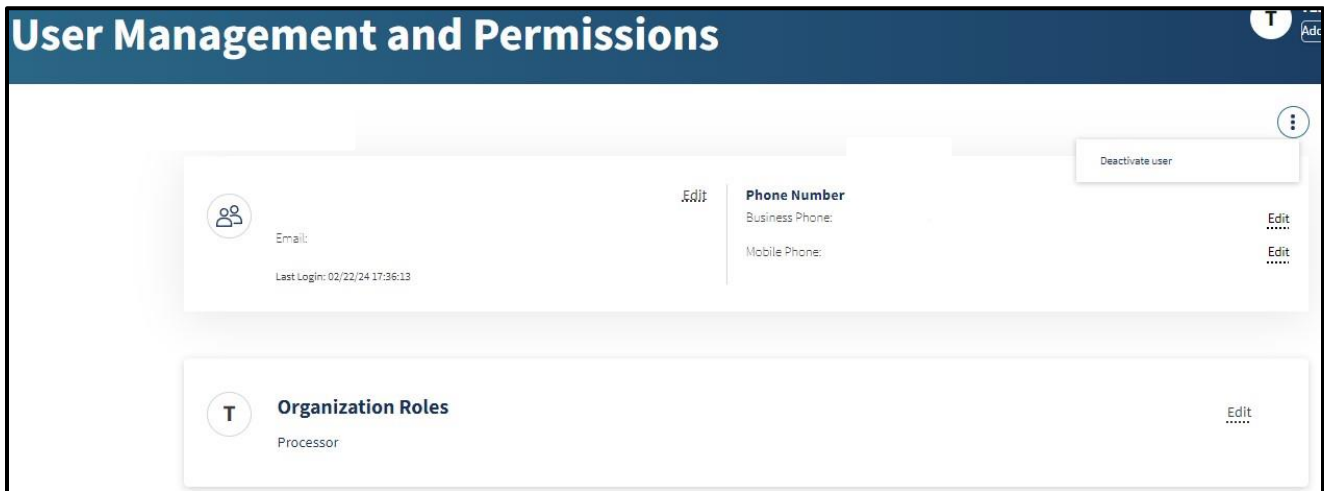1. Click the kebab menu in the far right and select **Deactivate User**.

Figure 2.28: User Management and Permissions.

2. A pop-up screen will appear asking for confirmation to deactivate the user. Click **Confirm**.

Are you sure you want to deactivate this user?

Deactivating this user will remove them from this organization. This will not remove any assets attached to their account or delete their access or other organizations.

Cancel   Confirm
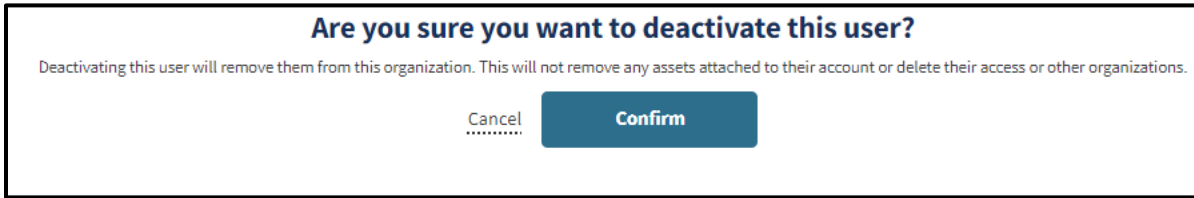
Figure 2.29: Deactivate User Confirmation.

3. Once complete, a successfully deactivated notification will appear within the **User Management and Permissions** profile of the user.

User successfully deactivated

Deactivated User

Email:

Last Login: 02/22/24 17:36:13

Edit

Phone Number

Business Phone: f

Mobile Phone:

Edit

Edit

Organization Roles

Processor

Edit
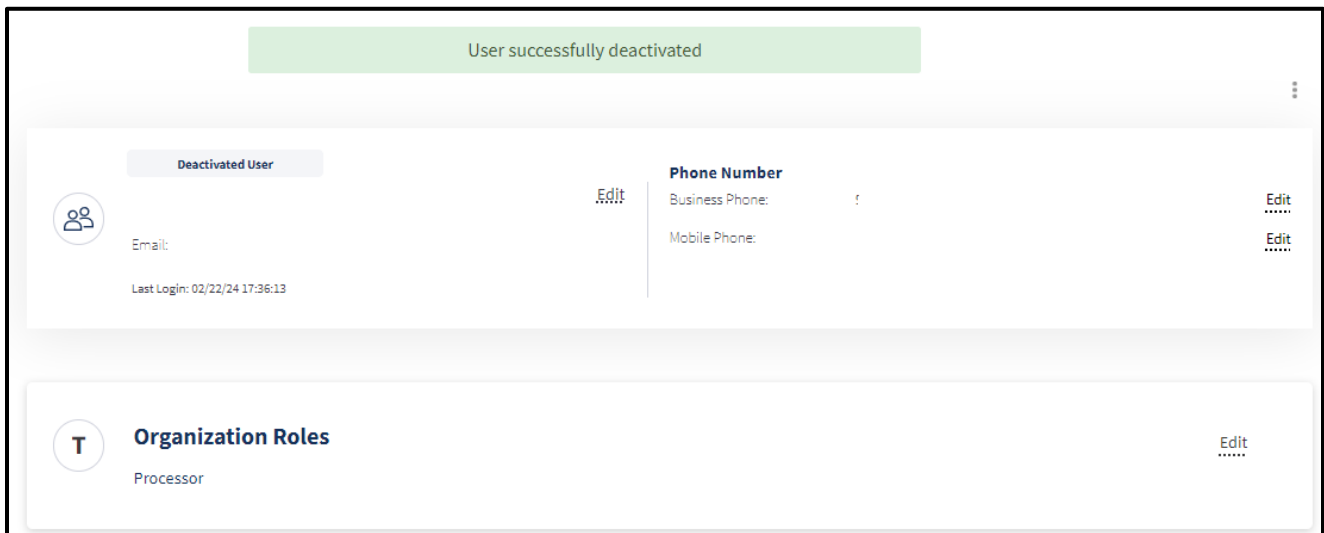
Figure 2.30: User Management and Permissions.

Notifications

The **Notifications** area allows a user to quickly view notifications related to their organization. The most recent notifications appear on the **Dashboard**. To see all notifications, click **View All**.
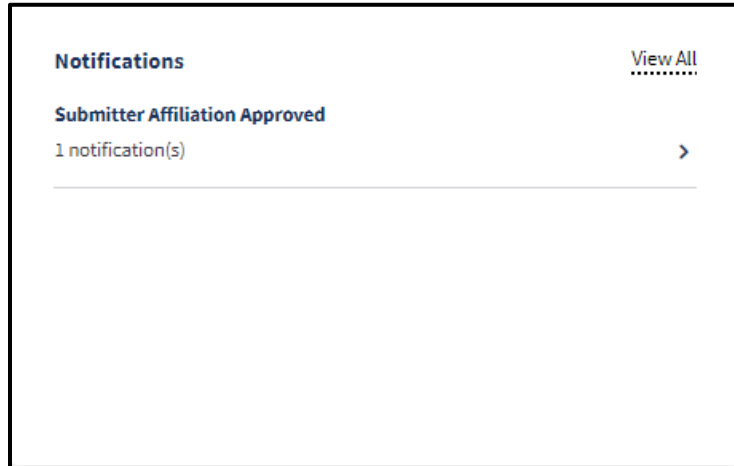
Figure 2.31: Notifications Tile.

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.
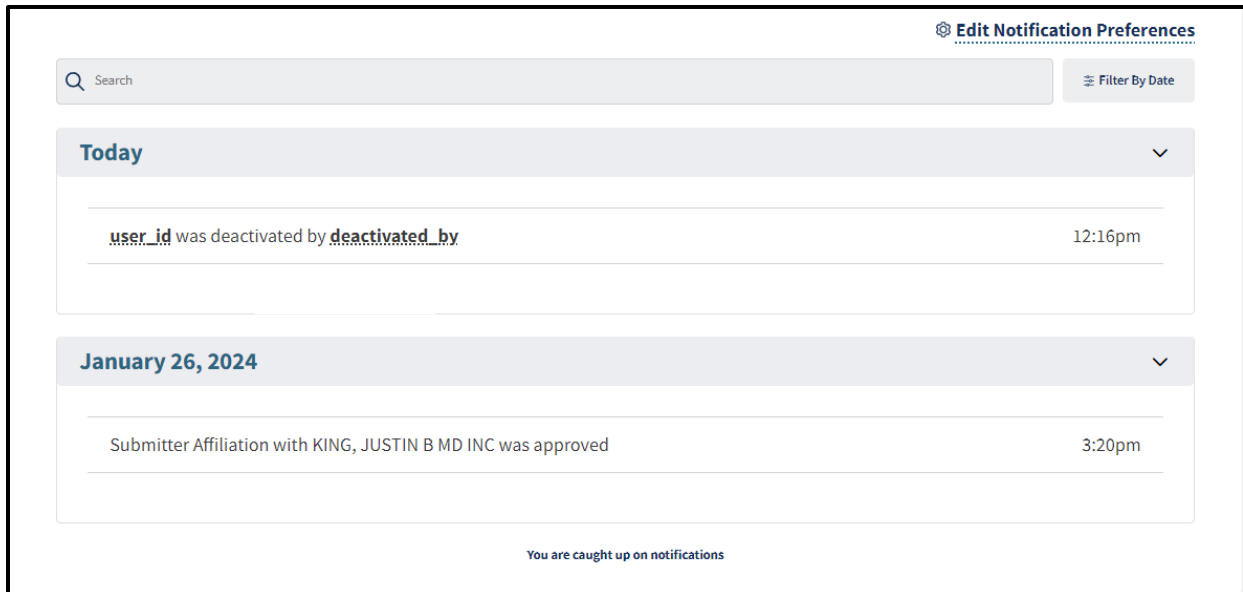
Figure 2.32: Notifications.

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

Provider Network

The Provider Organizations that submitters are affiliated with are viewable in **Provider Network** on the **Dashboard**. This area may only be accessed by individuals who are designated as organization admins.

Administrators can click **View All** to view **Pending Requests, Affiliations, Submitter Directory Profile** and to request a new affiliation:

1. Click **View All** to see all provider affiliations and requests
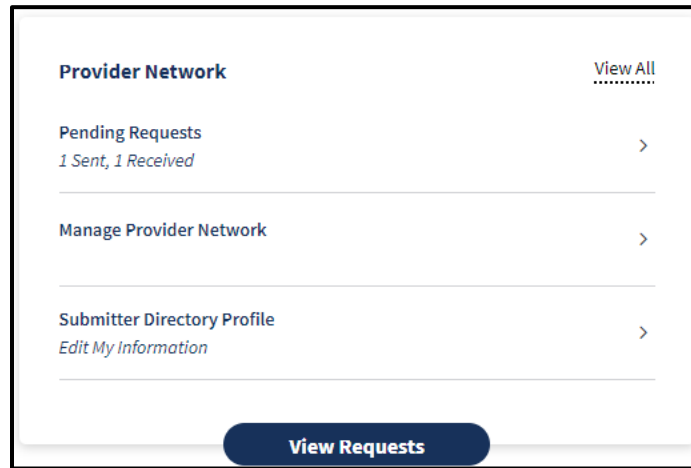
Figure 2.33: Provider Network Tile.

2. The **Pending Requests** tab displays the organizations where the status for affiliation is either Request Pending, Pending Approval or Expired. Affiliation requests are valid for 60 days and once it has expired the submitter organization can click **Re-Submit Request** to resend the affiliation request.
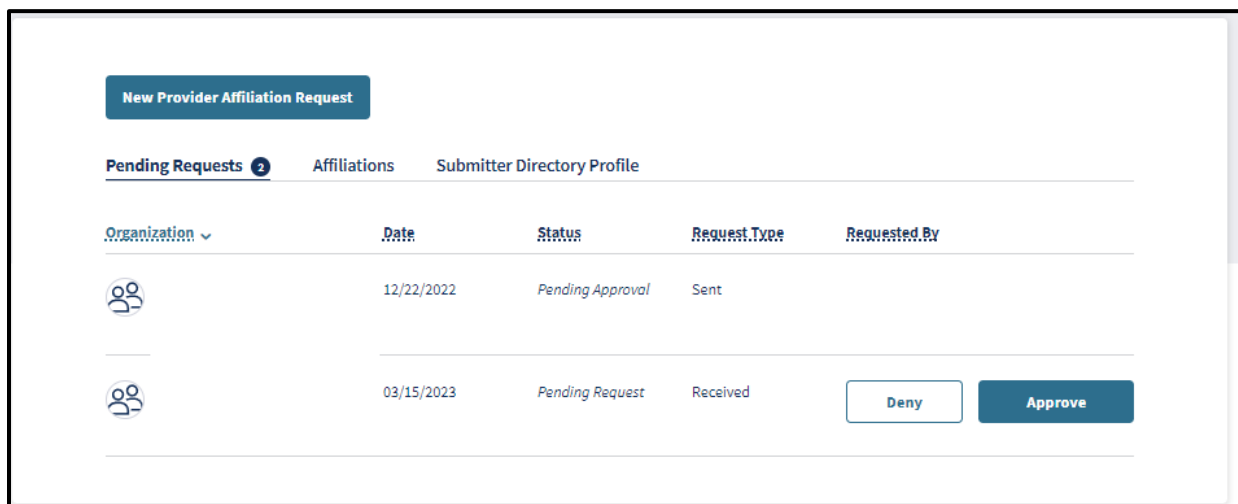
Figure 2.34: Pending Requests.

57

3. The **Affiliations** tab displays organizations where the status of the affiliation is Active or Inactive.

Figure 2.35: Affiliations.

4. The **Submitter Directory Profile** tab displays submitter ID, transaction types and contact information.

Figure 2.36: Submitter Directory Profile.
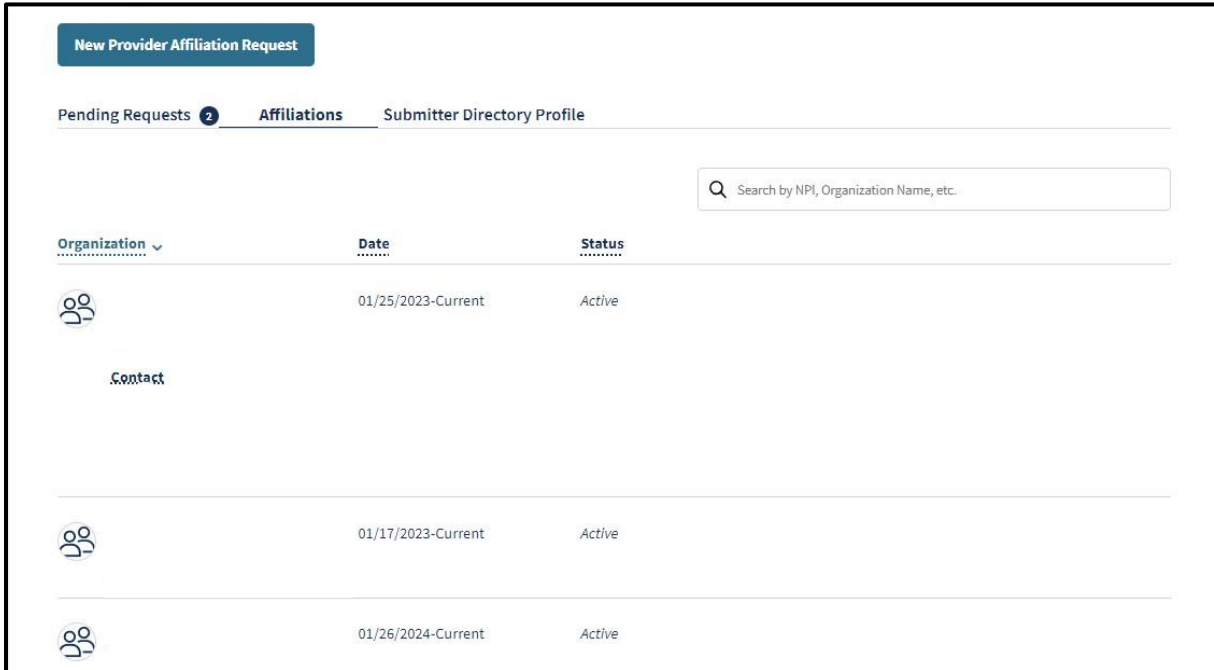
Note The green check mark will indicate that a submitter organization is listed in the submitter directory. To opt-out, view Edit Submitter Directory Information.

New Provider Affiliation Request

1. To request a new provider affiliation, click **New Provider Affiliation Request** within **Provider Network**.

Figure 2.37: Pending Requests.

2. An **Organization Information** screen will appear. Enter in the **Provider Tax ID** or **SSN** and the provider's **NPI**, then click **Next**.

Figure 2.38: Affiliation Provider Organization Information.

3. A screen for the *Medi-Cal Telecommunications Provider and Biller Application/Agreement* (DHCS 6153) form will appear. Please read the agreement form and then sign with First and Last name along with Title. Once complete, select **Submit Agreement**.

Figure 2.39: Medi-Cal Telecommunications Provider and Biller Application/Agreement.

4. A **Request Complete** screen will appear.

Figure 2.40: Request Complete.

Approve Provider Affiliation Request

1. Under the Pending Requests, click **Approve** for the desired provider organization affiliation request.
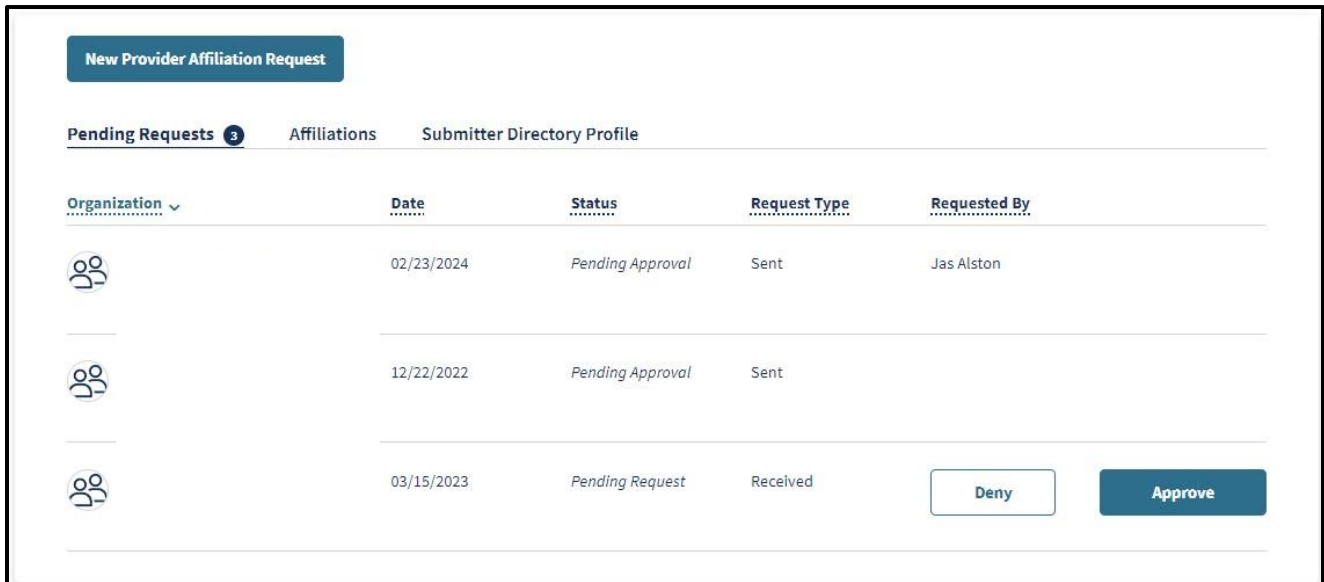

Figure 2.41: Pending Requests.

2. A screen for the *Medi-Cal Telecommunications Provider and Biller Application/Agreement* (DHCS 6153) form will appear. Please read the agreement form and then sign with First and Last name along with Title. Once complete, select **Submit Agreement**.

Figure 2.42: Medi-Cal Telecommunications Provider and Biller Application/Agreement.

3. Once complete, an **Approval Complete** screen will appear. Click **Return to Provider Network** to view active affiliations.
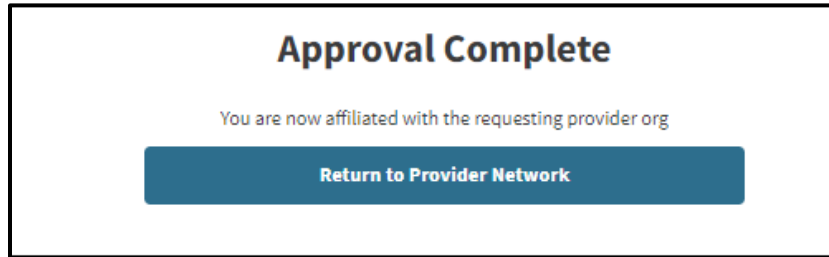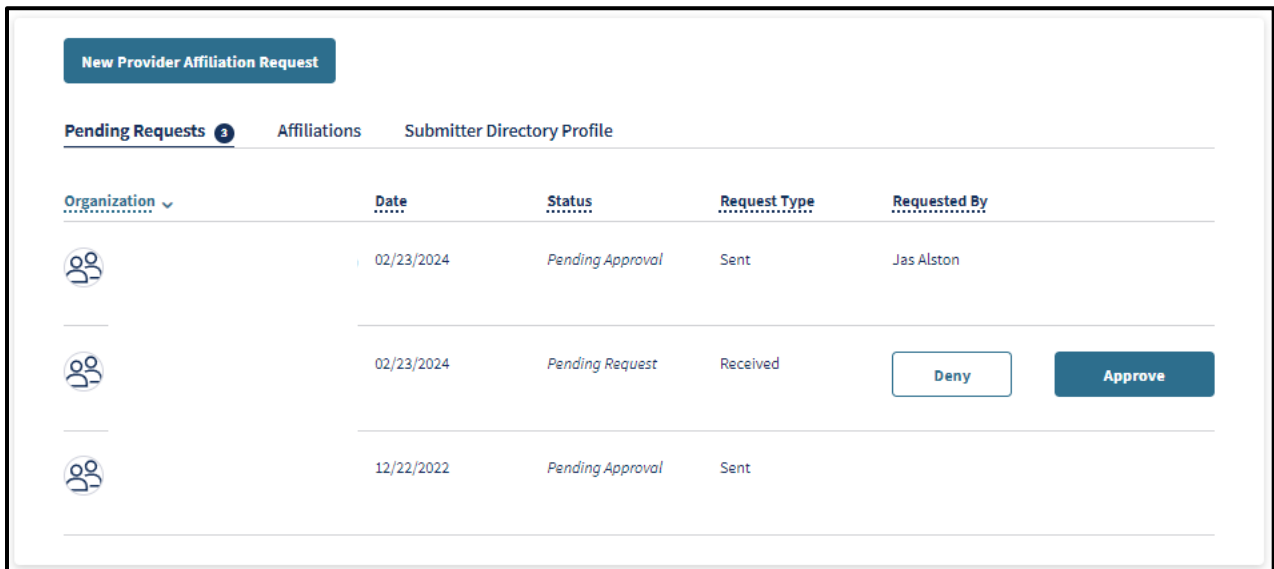

Figure 2.43: Approval Complete.

Note: Once an affiliation is approved, the provider organization can select the Medical claim type for the submitter organization prompting automatic enrollment in IPCS.

Deny Provider Affiliation Request

1. Under the Pending Requests, click **Deny** for the desired provider organization affiliation request.

Figure 2.44: Pending Requests.

2. A pop-up screen asking for confirmation to deny request will appear. Click **Deny** to continue.
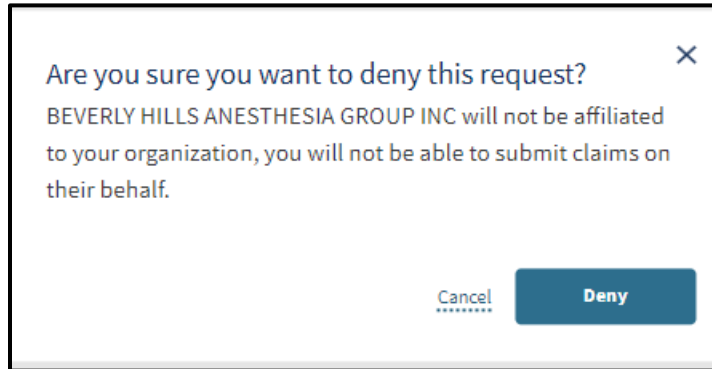

Figure 2.45: Deny Request Confirmation.

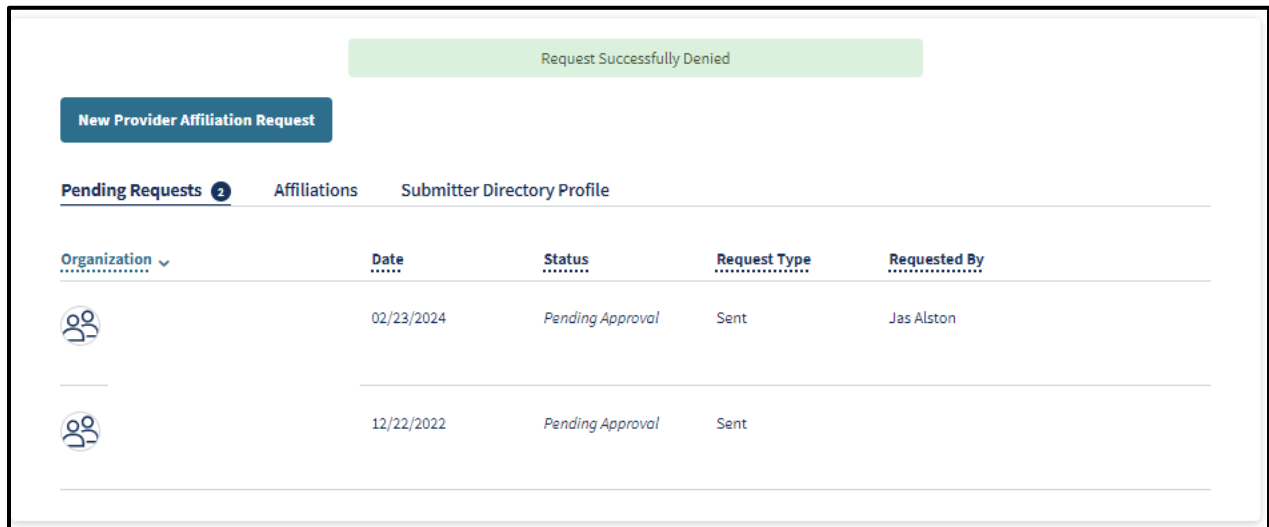3. Once complete, a successfully denied notification will appear within the **Provider Network**.

Figure 2.46: Request Successfully Denied.

Remove Provider Affiliation

1. To remove a provider affiliation from the **Provider Network**, select the desired Provider Organization listed under Affiliations.
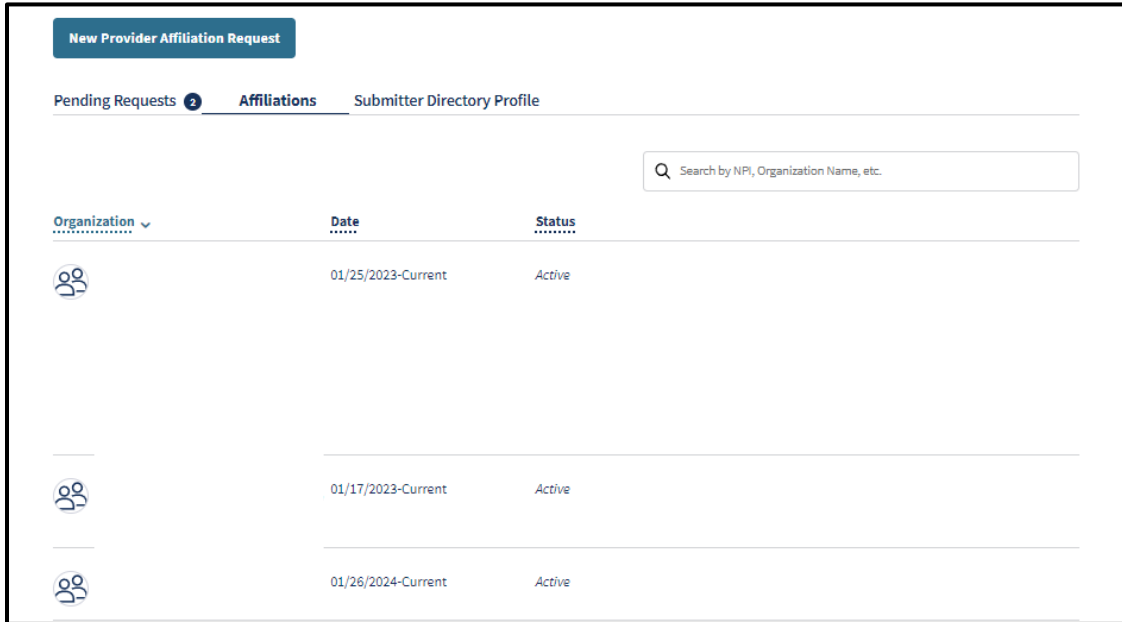

Figure 2.47: Affiliations.

2. The provider organization's profile will appear within the **Provider Network**.
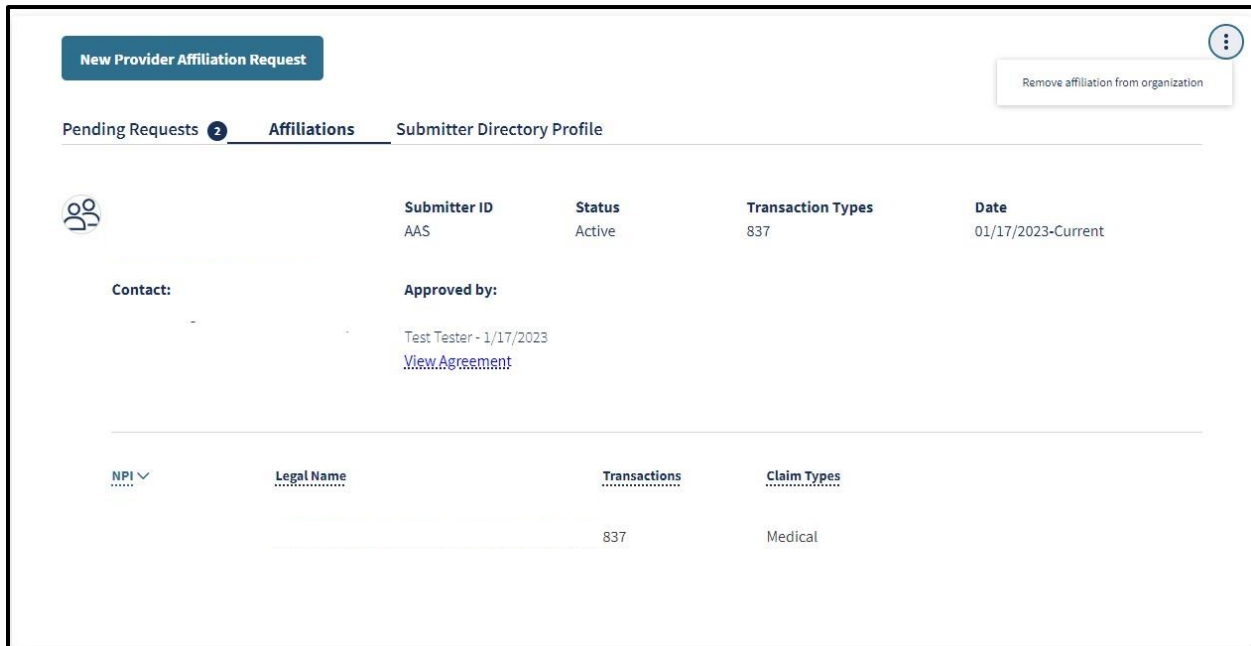
Figure 2.48: Affiliated Provider Organization Profile.

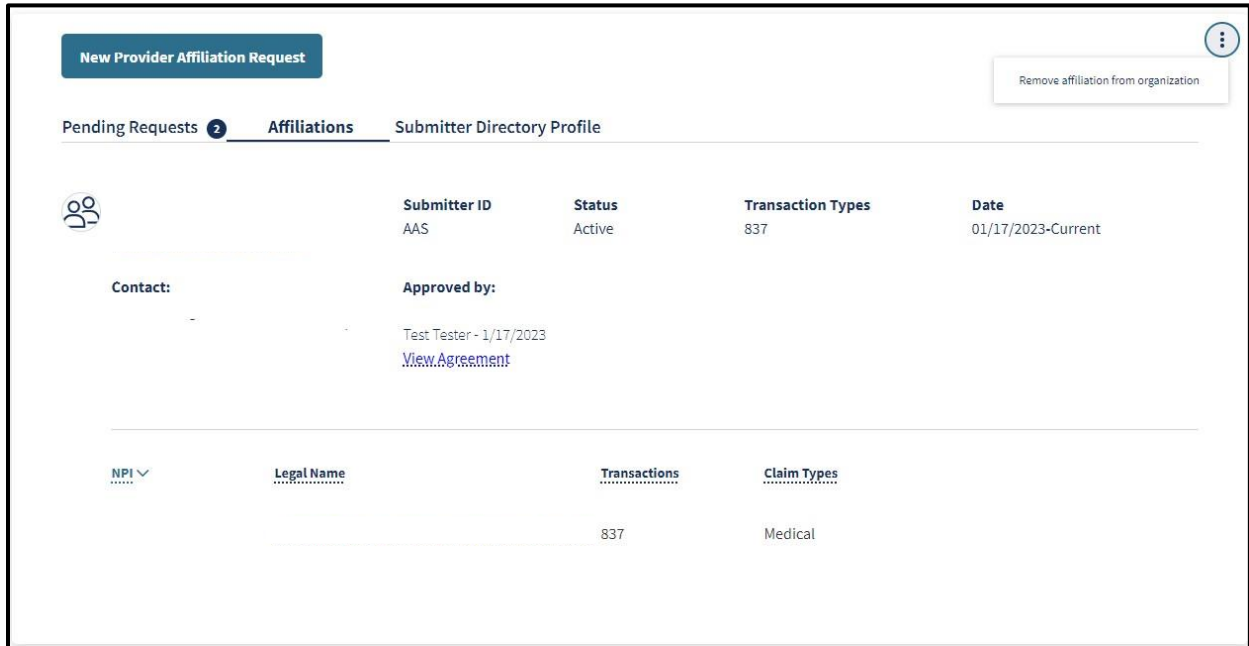3. Select the kebab menu in the top right-hand corner and then click **Remove affiliation from organization**.

Figure 2.49: Remove Affiliation From Organization.

4. A screen will appear to confirm the removal of the affiliation. Please type the organization's name in the field below to verify and click **Yes, remove the affiliation**.
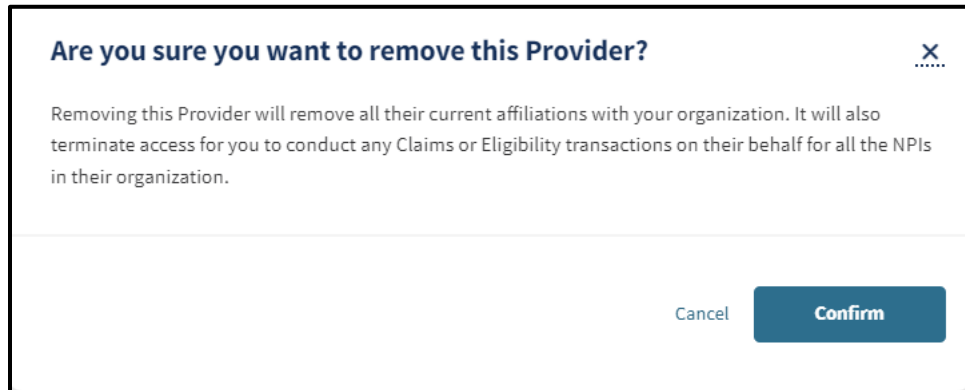
Figure 2.50: Remove Affiliation.

5. A notification stating, "Affiliation removed successfully," will appear within Provider Network and the status of the organization will read "Inactive."

Figure 2.51: Affiliation Removed Successfully.

Medi-Cal 835 Receiver

The Provider Portal allows only provider 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.

Submitter organizations designated to be an 835 receiver will receive a notification within the Provider Portal after being added by an organizational NPI.
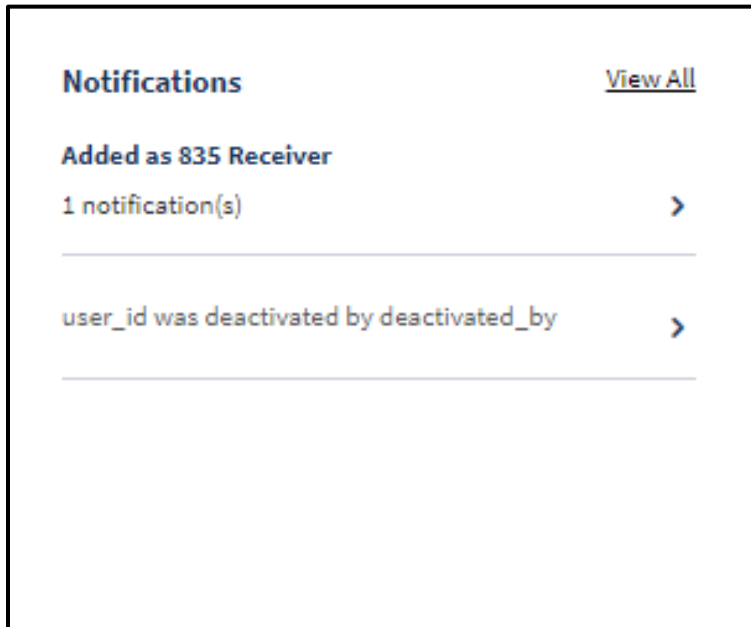
Figure 2.52: 835 Receiver Notification.

Transaction Testing

The **Transaction Testing** area allows users to submit transaction testing for Claims 837 and Eligibility Benefit 270/271 transactions. The user can also view the status of each **Transaction Type** and the Date of Completion. The status of each Transaction Type will report as Not Started, Pending or Active.

1. To view testing status, select **View All** within the **Transaction Testing** tile of the **Dashboard**.
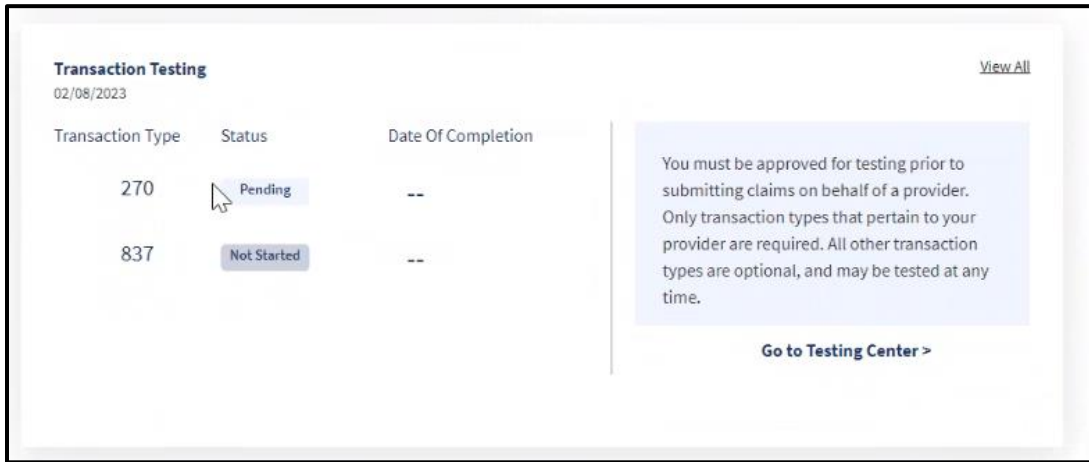
Figure 2.53: Transaction Testing Tile.

2. The **Submitter Testing Status** will appear for the each of transaction types available.
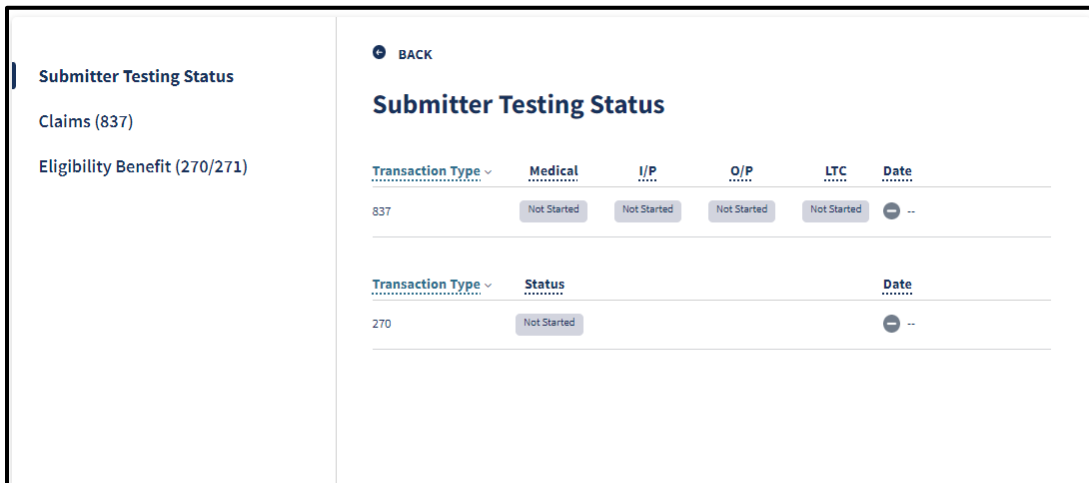
Figure 2.54: Submitter Testing Status.

Claims 837 Transaction Testing

1. Select **Claims (837)** under **Submission Management**. Click **Upload a Submission.**
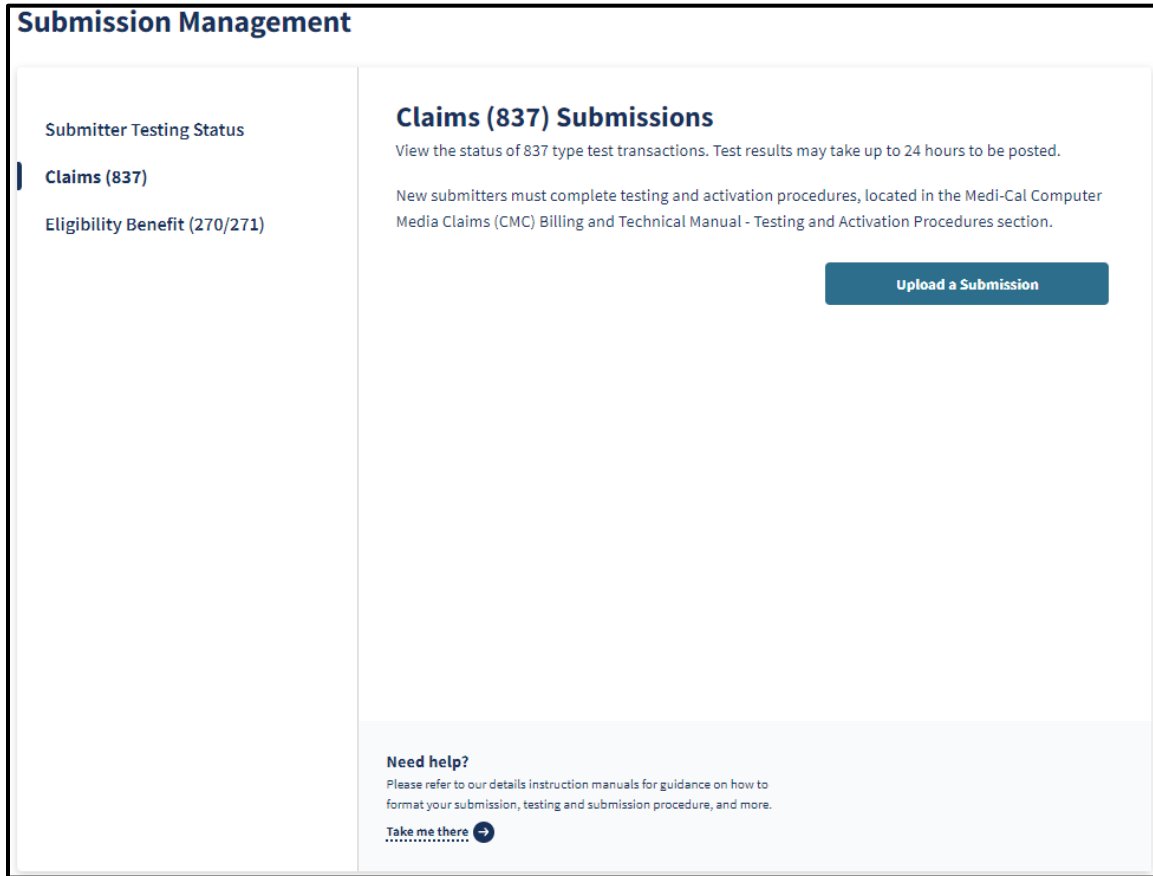
Figure 2.55: Claims (837) Submissions.

2. Select **Drag and drop your files here or click to browse** to upload a file for claim type approval. If approved, submitters will be able to submit the claim type for valid providers and the test results will be received within 24 hours.
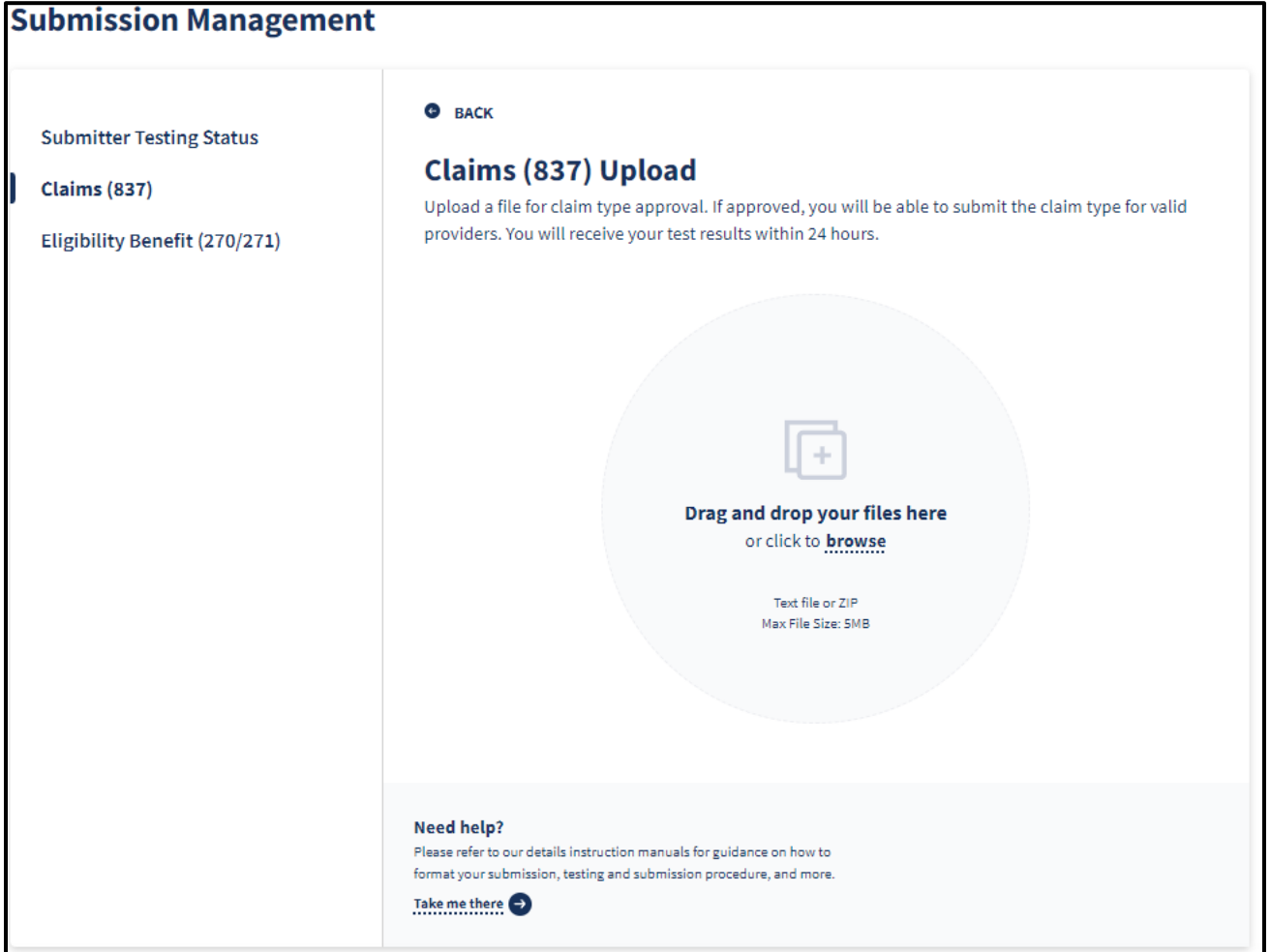
Figure 2.56: Claims (837) Upload.

3. Complete will appear on the screen once the file has been uploaded.
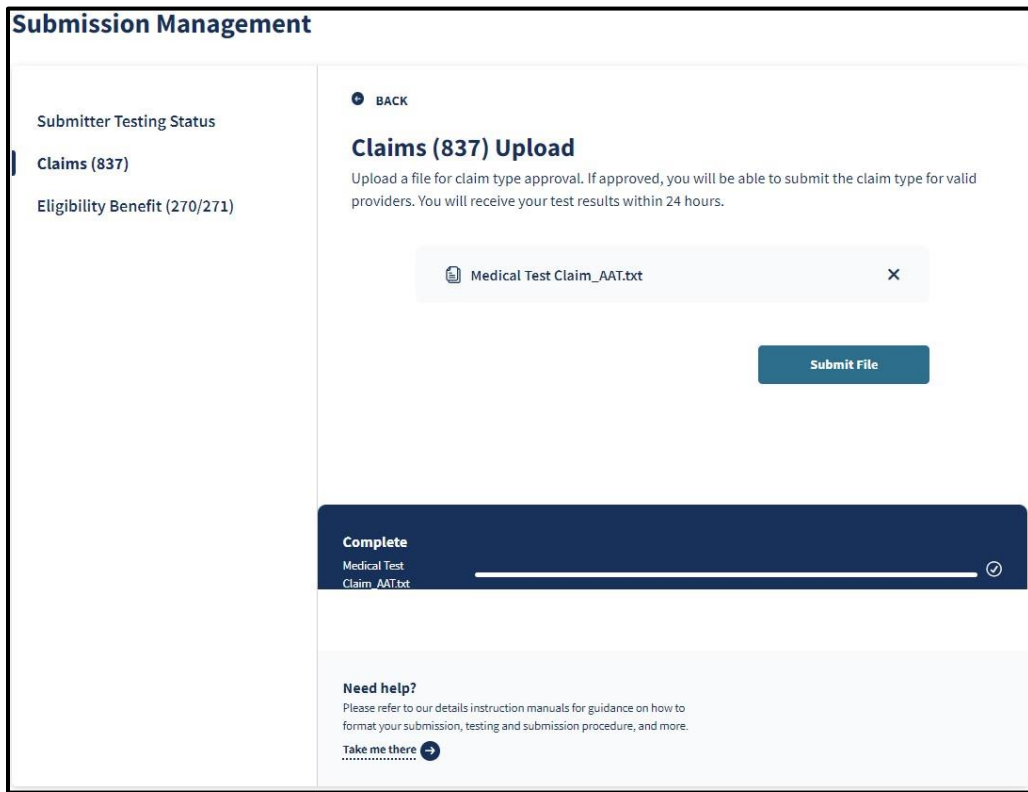
Figure 2.57: Claims (837) Upload Complete.

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

Figure 2.58: Upload Another File.

5. Select **Claims (837)** to view the status of each test file. Each uploaded file will be issued a Volser number.

Figure 2.59: Claims (837) Submissions.

Note: Volser details may not be available for up to 24 hours after the submission is uploaded, and details are available for approximately 30 days.

6. Once a Passed status appears for the Volser number, the **Account Status** bar will update with a green check mark for **Complete transaction testing**.
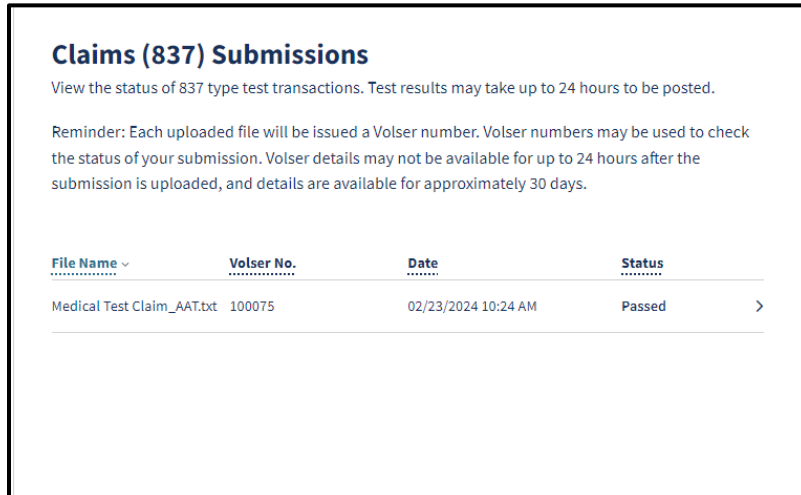

Figure 2.60: Complete Transaction Testing Account Status.

7. Select the **Volser number** with the passed status and view the details of the test submission.
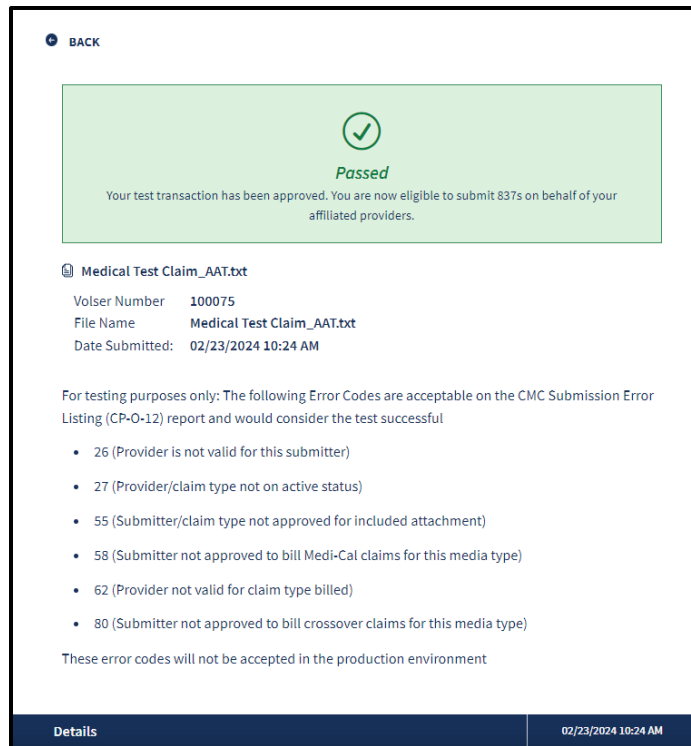

Figure 2.61: Claims (837) Submissions.

8. A submitter is ready to submit 837 claims once the test has passed.

Figure 2.62: Passed Transaction Testing.

9. Select the **Volser number** with the failed status and view the details of the test submission.

Figure 2.63: Claims (837) Submissions.

10. A submitter must resubmit the test transaction in order to until it has passed in order to submit 837 claims.

Figure 2.64: Failed Transaction Testing.

Eligibility Benefit 270 Transaction Testing

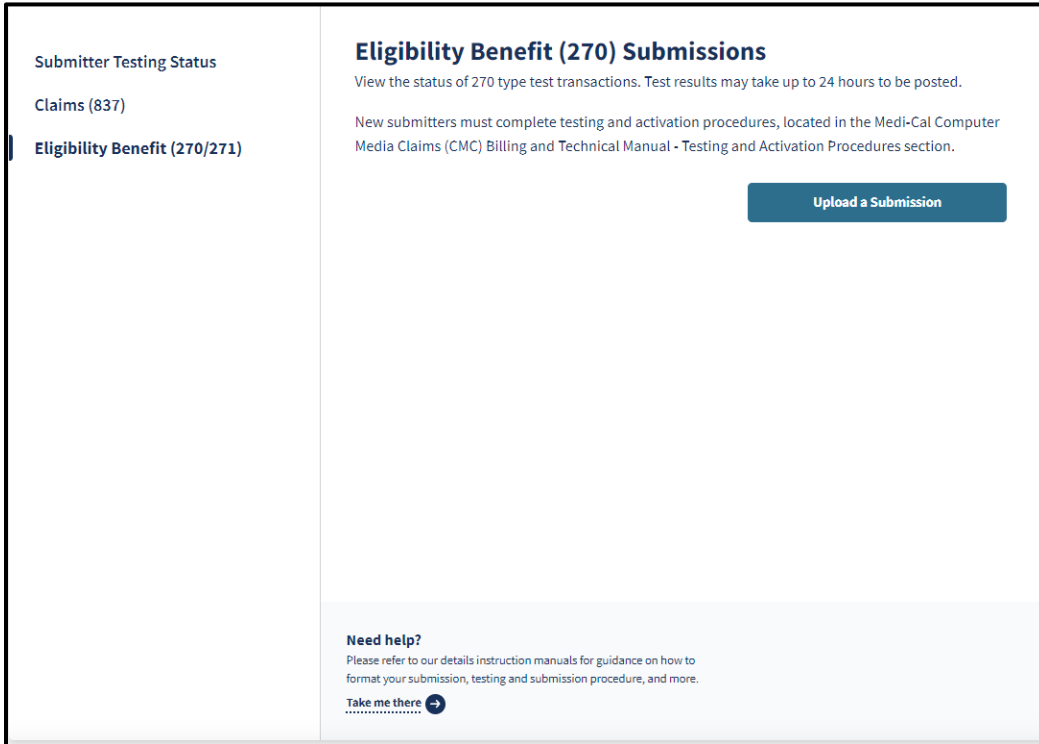1. Select **Eligibility Benefit (270/271)** under Submission Management. Click **Upload a Submission**.

Figure 2.65: Eligibility Benefit (270) Submissions.

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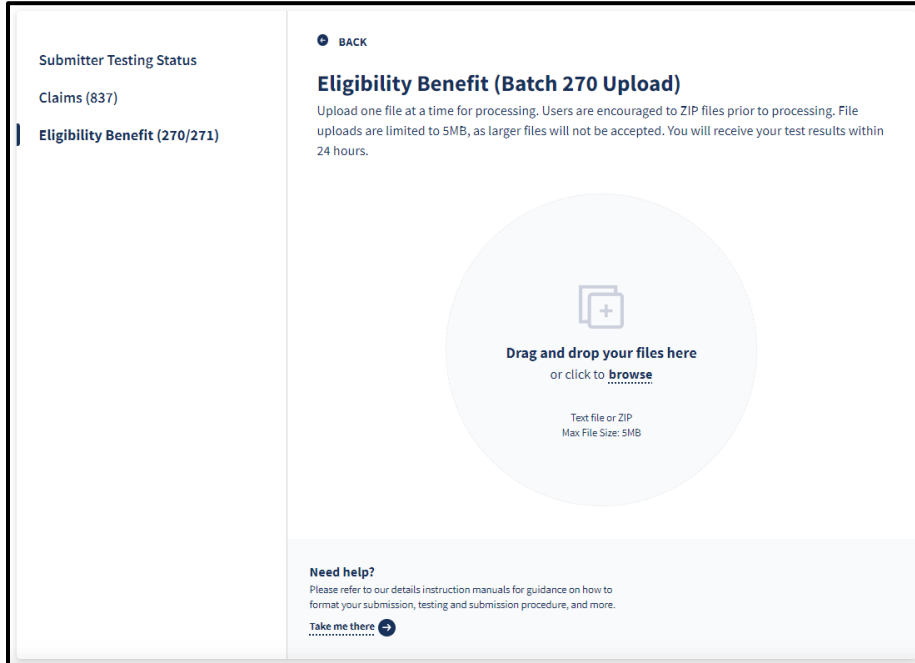

Figure 2.66: Eligibility Benefit (Batch 270 Upload).

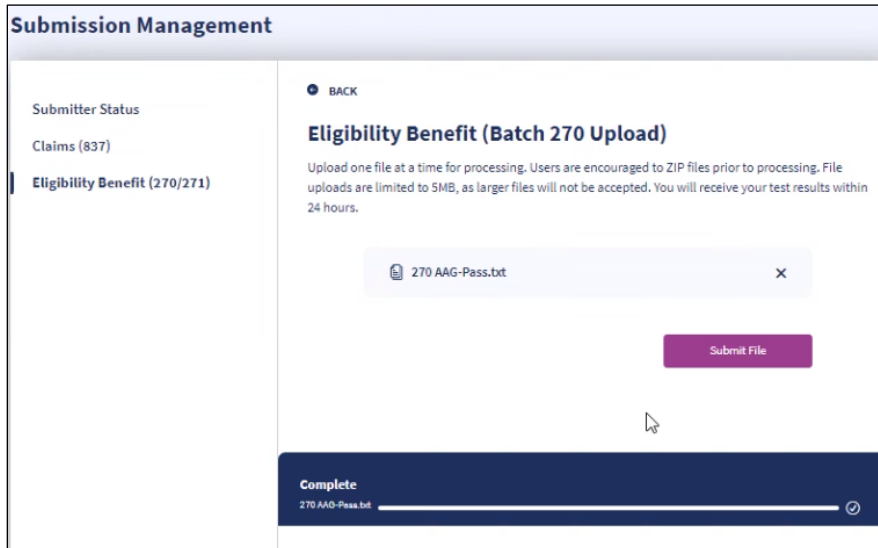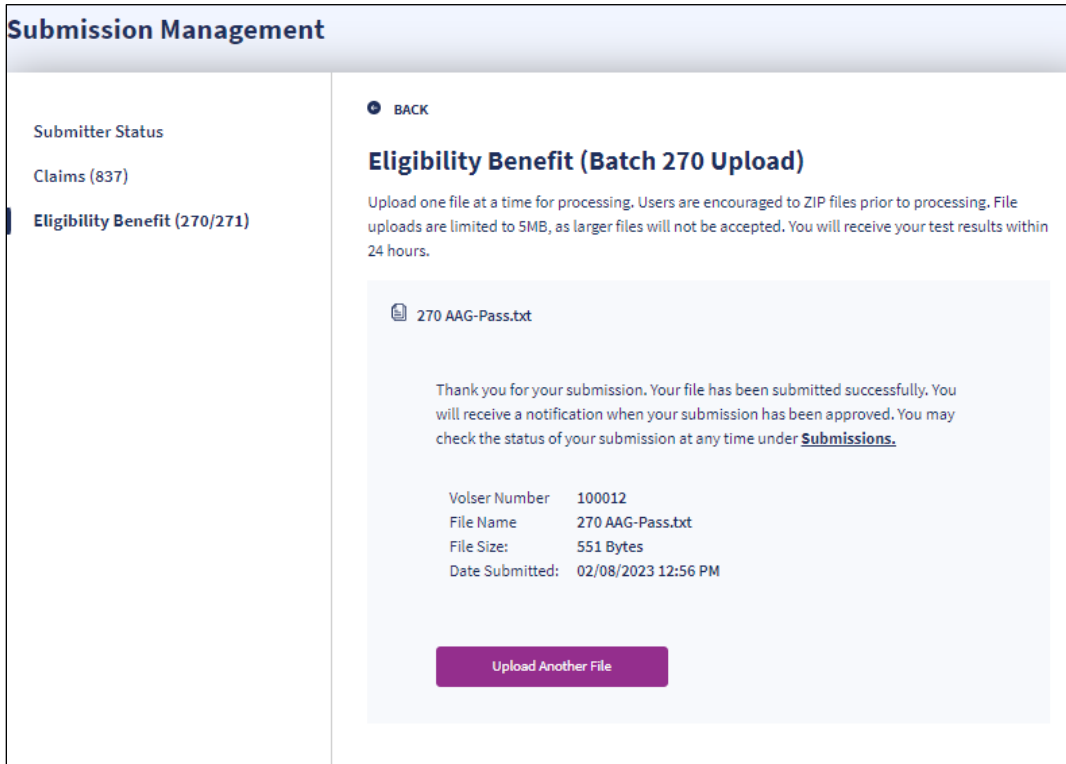3. Complete will appear on the screen once the file has been uploaded.

Figure 2.67: Eligibility Benefit (Batch 270 Upload) complete.

4. Once the file is successfully uploaded, the Volser Number, File Name, File Size and Date Submitted will appear.

Figure 2.68: Upload Another File.

5. Select **Eligibility Benefit (270/271)** to view the status of each test file. Each uploaded file will be issued a Volser number

Figure 2.69: Eligibility Benefit (Batch 270 Upload) Submissions.

Note: Volser details may not be available for up to 24 hours after the submission is uploaded, and details are available for approximately 30 days.

6. Once a Passed status appears for the Volser number, the **Account Status** bar will update with a green check mark for **Complete transaction testing**.

Figure 2.70: Complete Transaction Testing Account Status Bar.

7. Submitters 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 on the testing acknowledgments.

Change Summary

Version Number	Date	Description	Notes/Comments
1.1	July 28, 2023	Associated with SDN 20015B	Updated screenshots and instructions to include 835 Receiver Management. Updated User Guide format.
1.2	March 15, 2024	Associated with SDN 20015B	Updated screenshots to match the new DHCS rebranding and the Transaction Center functions.
1.3	September, 2024	Associated with SDNs 20015B and 23036	Updated screenshot to include the new Passkey and Unlock Password features in Provider Portal. Also, updated the DHCS logo on the cover page. Update formatting.