# Revision History

<table>
<thead>
<tr>
<th>Version #</th>
<th>Date of Release</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>04/03/2018</td>
<td>Initial Version</td>
</tr>
<tr>
<td>2.0</td>
<td>05/07/2018</td>
<td>Final Version</td>
</tr>
</tbody>
</table>
Table of Contents

Revision History ............................................................................................................................................ 2
Table of Contents ........................................................................................................................................ 3
Table of Figures .......................................................................................................................................... 5

1 Introduction ............................................................................................................................................ 8
  1.1 Purpose ...................................................................................................................................... 8
2 Denti-Cal's Provider Website Landing Home Page .................................................................................... 8
3 Registration on Provider Portal .............................................................................................................. 9
  3.1 Steps for Registration: Positive Scenario ................................................................................... 9
  3.2 Steps to Register with Validations ........................................................................................... 13
    3.2.1 Scenario 1: The Provider Enters Incorrect Details .................................................................. 13
    3.2.2 Scenario 2: If user enters combination of First Name, Last Name and Email Address same as that of an already registered user and tries to register ........................................................................ 19
    3.2.3 Scenario 3: If user left any/all of the required fields blank .................................................... 20
    3.3 Username Reminder Steps ...................................................................................................... 20

4 Provider Secure Log In .......................................................................................................................... 23
  4.1 Account Unlock Flow ............................................................................................................... 24
    4.1.1 Scenario 1: Provider is successful in unlocking account by answering only 1 security question .................................................................................................................................. 24
    4.1.2 Scenario 2: If Provider answers the 1st Security Question incorrectly ................................... 26
    4.1.3 Scenario 3: If Provider’s Username is not verified ................................................................. 27
    4.1.4 Scenario 4: If a Provider is unable to unlock their account by entering invalid security answers for both questions........................................................................................................... 27
  4.2 Password Reset Flow ............................................................................................................... 28
    4.2.1 Scenario 1: A Provider successfully resets their password by answering only 1 security question .................................................................................................................................. 28
    4.2.2 Scenario 2: When Providers successfully reset their password by answering the 2nd security question correctly ..................................................................................................... 32
    4.2.3 Scenario 3: If Providers are unable to reset their password ..................................................... 33
    4.2.4 Scenario 4: When a provider’s password expires ................................................................... 34
    4.2.5 Scenario 5: If Provider enters an invalid password ................................................................ 35

5 Denti-Cal Provider Website Tabs .......................................................................................................... 37
  5.1 My Practice Tab ....................................................................................................................... 37
  5.2 Claim/TAR Tab .......................................................................................................................... 41
  5.3 Payments ...................................................................................................................................... 42
    5.3.1 Scenario 1: When provider enters correct PIN. ................................................................. 42
    5.3.2 Scenario 2: When provider enters an incorrect PIN ........................................................... 43
  5.4 Account Tab .................................................................................................................................. 44
    5.4.1 Scenario 1: If a Provider is an Administrator (Admin) ............................................................ 44
    5.4.2 Scenario 2: When a provider is a Regular User ................................................................. 45
    5.4.3 Scenario 3: Successfully changing Password from the Accounts Page .............................. 46
    5.4.4 Scenario 4: When a Provider successfully updates their password – Account tab ............ 47
5.4.5 Scenario 5: When a Provider is unable to update their password through the Account tab.

6 Admin Functionality Features

6.1 Manage Users

6.1.1 Add User

6.1.1.1 Scenario 1: If Provider enters details with same combination of First Name, Last Name and Email of an already added user.

6.1.1.2 Scenario 2: If Provider enters invalid details.

6.1.1.3 When an added user tries to register.

6.1.2 Edit Users

6.1.2.1 Scenario 1: If provider enters invalid details.

6.1.3 Delete Users

7 Reporting a Missed Appointment Feature

7.1 Scenario 1: If Provider enters invalid details in the Missed Appointment Form.

8 Provider Resources

9 Contact Us Page
Table of Figures

<table>
<thead>
<tr>
<th>Fig:</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.a</td>
<td>Denti-Cal's Provider Website Landing Home Page</td>
</tr>
<tr>
<td>3.1.a</td>
<td>Denti-Cal's Provider Website Login Page – Registration Link</td>
</tr>
<tr>
<td>3.1.b</td>
<td>Verify User Registration Page</td>
</tr>
<tr>
<td>3.1.c</td>
<td>Create Account Registration Page</td>
</tr>
<tr>
<td>3.1.d</td>
<td>Registration Completed Successfully Message Screen</td>
</tr>
<tr>
<td>3.1.e</td>
<td>Welcome Email with Privacy Policy Link after Successful Provider Registration</td>
</tr>
<tr>
<td>3.1.f</td>
<td>User Details not validated during Registration</td>
</tr>
<tr>
<td>3.1.g</td>
<td>Error Message for Entering Invalid Username while Creating Account</td>
</tr>
<tr>
<td>3.1.h</td>
<td>Error Message for Entering Invalid Email Address while Creating Account</td>
</tr>
<tr>
<td>3.1.i</td>
<td>Error Message for Entering Invalid Password while Creating Account</td>
</tr>
<tr>
<td>3.1.j</td>
<td>Error Message for Entering Incorrect Password in Confirm Password Field while Creating Account</td>
</tr>
<tr>
<td>3.1.k</td>
<td>Error Message for not selecting the Check Box to Agree to the Terms and Conditions</td>
</tr>
<tr>
<td>3.1.l</td>
<td>Error Message for Selecting the Same Security Question during Account Creation</td>
</tr>
<tr>
<td>3.1.m</td>
<td>Error Message for not selecting the CAPTCHA while Creating User Account</td>
</tr>
<tr>
<td>3.2.1.n</td>
<td>Username Reminder Link</td>
</tr>
<tr>
<td>3.2.3.p</td>
<td>Error Message when Fields Left Blank during Registration</td>
</tr>
<tr>
<td>3.3.q</td>
<td>Username Reminder Screen</td>
</tr>
<tr>
<td>3.3.r</td>
<td>Username Reminder Message</td>
</tr>
<tr>
<td>3.3.s</td>
<td>Email Sent to the Provider for Username Reminder</td>
</tr>
<tr>
<td>4.a</td>
<td>Unable to Login Error – when Provider Tries to Log In with Invalid Credentials</td>
</tr>
<tr>
<td>4.b</td>
<td>Account Locked Message – when Provider Exceed the Maximum Login Attempts</td>
</tr>
<tr>
<td>4.1.1.c</td>
<td>Unlock Account Screen to Validate Credentials – Provider to Enter Username</td>
</tr>
<tr>
<td>4.1.1.d</td>
<td>Unlock Account Screen to Validate User – Security Question</td>
</tr>
<tr>
<td>4.1.1.e</td>
<td>Provider Account Unlocked Successfully</td>
</tr>
<tr>
<td>4.1.2.f</td>
<td>Unlock Account Screen to Validate User – Second Security Question</td>
</tr>
<tr>
<td>4.1.3.g</td>
<td>Unlock Account Screen to Validate User – Incorrect Username Entered</td>
</tr>
<tr>
<td>4.1.4.h</td>
<td>Unlock Account Screen – Unable to Validate User, Send Email to Unlock Account</td>
</tr>
<tr>
<td>4.2.i</td>
<td>Provider Website Landing Page – Reset Password Link</td>
</tr>
<tr>
<td>4.2.1.j</td>
<td>Reset Password – Provider Identification by Entering Username</td>
</tr>
<tr>
<td>4.2.1.k</td>
<td>Reset Password – Provider Verification by Entering Answer for Security Question</td>
</tr>
<tr>
<td>4.2.1.l</td>
<td>Reset Password – Mail sent to User Message Screen</td>
</tr>
<tr>
<td>4.2.1.m</td>
<td>Reset Password Link in an Email Sent to the Provider</td>
</tr>
<tr>
<td>4.2.1.n</td>
<td>Reset Password Page</td>
</tr>
<tr>
<td>4.2.2.o</td>
<td>Message – Password Updated Successfully after Provider Resets the Password</td>
</tr>
<tr>
<td>4.2.2.p</td>
<td>Reset Password – Provider to Answer 2nd Security Answer</td>
</tr>
<tr>
<td>4.2.3.q</td>
<td>Reset Password – User Unable to Reset Password Screen</td>
</tr>
<tr>
<td>4.2.4.r</td>
<td>Change Password Screen</td>
</tr>
<tr>
<td>4.2.4.s</td>
<td>Password Successfully Updated</td>
</tr>
<tr>
<td>4.2.5.t</td>
<td>Reset Password Error – Password Entered is Invalid</td>
</tr>
<tr>
<td>4.2.5.u</td>
<td>Reset Password Error – Password and Confirm Password do not Match</td>
</tr>
</tbody>
</table>
Passwords ................................................................................................................................................... 36
Fig: 5.1.a: Provider Website – My Practice Tab – Change Location ............................................................. 37
Fig: 5.1.b: Provider Website – My Practice Tab – Change and Select Location ....................................... 38
Fig: 5.1.c: Provider Website – My Practice Tab, Claim/TAR Link ............................................................ 38
Fig: 5.1.d: Provider Website – My Practice Tab – Individual Claim/TAR Details ...................................... 39
Fig: 5.1.e: Provider Website – My Practice Tab – Check/EFT – Enter PIN Screen .................................... 39
Fig: 5.1.f: Provider Website – My Practice Tab – Check/EFT – PIN not Valid Screen ............................... 40
Fig: 5.2.g: Provider Website – Claim/TAR Tab .......................................................................................... 41
Fig: 5.3.1.h: Provider Website – Payments Tab – Enter PIN ................................................................... 42
Fig: 5.3.1.i: Provider Website – Payments Tab – Payment History ......................................................... 42
Fig: 5.3.2.j: Provider Website – Payments Tab – Check/EFT# ................................................................. 43
Fig: 5.3.2.k: Provider Website – Payments Tab – PIN not Valid ............................................................... 43
Fig: 5.4.1.l: Provider Website – Account Tab – Admin User ................................................................. 44
Fig: 5.4.2.m: Provider Website – Account Tab – Regular User ............................................................... 45
Fig: 5.4.3.n: Provider Website – Account Tab – Change Password Button ............................................ 46
Fig: 5.4.4.p: Provider Website – Account Tab – Password updated successfully .................................... 48
Fig: 5.4.5.q: Provider Website – Account Tab – If new password same as current password ............... 48
Fig: 5.4.5.r: Provider Website – Account Tab – If new password is the same as the 24 previously used passwords ................................................................................................................................................... 49
Fig: 5.4.5.s: Provider Website – Account Tab – If New Password and Confirm Password do not match ................................................................................................................................................... 49
Fig: 5.4.5.t: Provider Website – Account Tab – If New Password does not conform to the Password Rules ................................................................................................................................................... 49
Fig: 6.1.a: Provider Website- Account Tab – Manage User Tab ............................................................ 50
Fig: 6.1.b: Provider Website – Manage User Page .................................................................................. 50
Fig: 6.1.1.c: Provider Website – Add User Page ....................................................................................... 51
Fig: 6.1.1.d: Provider Website – Email Sent to the added User with a Registration Link .......................... 51
Fig: 6.1.1.e: Provider Website – Registration Page 1 for Added Users .................................................. 52
Fig: 6.1.1.f: Provider Website – User already exists while adding user .................................................. 53
Fig: 6.1.1.g: Provider Website – Invalid Details Entered while Adding User ......................................... 54
Fig: 6.1.1.2.h: Provider Website – Invalid Details Entered by Added User ............................................... 57
Fig: 6.1.2.k: Provider Website – Edit Button ............................................................................................ 56
Fig: 6.1.2.l: Provider Website – Edit User Page ........................................................................................ 56
Fig: 6.1.2.m: Provider Website – Edit User Page, Invalid Details Entered ............................................ 57
Fig: 6.1.3.n: Provider Website – Delete Button from User List ............................................................... 57
Fig: 6.1.3.o: Provider Website – Delete Button – Confirm Delete Pop Up ................................................ 58
Fig: 6.1.3.p: Provider Website – Updated List after Deleting a User ....................................................... 58
Fig: 7.a: Provider Website – Missed Appointment Link on the My Practice Page .................................. 59
Fig: 7.b: Provider Website – Missed Appointment Link on the My Practice Page ............................... 60
Fig: 7.c: Provider Website – Missed Appointment Link on the My Practice Page .................................. 61
1 Introduction

1.1 Purpose

This is a user guide for the Denti-Cal Provider Website Application.

2 Denti-Cal’s Provider Website Landing Home Page

Denti-Cal’s landing home page for providers has a secure log in for providers to register online. Every provider will have a unique account that will allow them to access multiple practice locations. The features on the landing home page are listed below (see Fig: 2.a).

- Username and Password field for Secure Log In
- Register Link
- Reset Password Link
- Username Reminder

Provider Website Landing Home Page:
3 Registration on Provider Portal

Denti-Cal providers can register themselves by clicking the “Register” link available on the Denti-Cal Provider Website Landing page. The first provider who registers for a particular Business Entity (Provider ID) will be assigned as an Administrator, by default, and will have special Administrator rights. Additional providers who register using the same Business Entity (Provider ID) will be “regular users” of the provider website and will be granted limited access.

3.1 Steps for Registration: Positive Scenario

Step 1:
Click the “Register” link (see Fig: 3.1.a).

![Fig: 3.1.a: Denti-Cal’s Provider Website Login Page – Registration Link]

Step 2:
The “Verify User │ Registration” page displays. A red asterisk (*) indicates a required field. Enter your information in the following required fields:

- Business Name as it appears on your Explanation of Benefits (EOB)
- Billing NPI Number
- TIN

The following fields are optional:

- Provider First Name
- Provider Last Name
Click the “Continue” button to continue the registration process. Click the “Cancel” button to close the page and return to the “Login” page (see Fig: 3.1.b).

![Verify User Registration Page](image)

**Step 3:**

After clicking the “Continue” button, the system goes to the next page in the registration process.

The systems populates the Provider Business Name, Billing NPI Number and Provider TIN entered in Step 2. The optional fields (Provider First Name and Provider Last Name) only populate if you entered the information in Step 2.

All the fields listed below are mandatory and must be completed (see Fig: 3.1.c).

- Username
- Email Address, Confirm Email Address
- First Name, Last Name
- Password, Confirm Password
- 2 Security Questions and Answers
- Check Box for the Terms and Conditions
- Check Box for CAPTCHA

The First Name, Last Name and Email Address fields are used for verification of the Username Reminder.
Fig: 3.1.c: Create Account Registration Page
Click the “Create” button to go to the “Registration Confirmation” page and view the “Registration Completed Successfully” message (see Fig: 3.1.d).

![Registration Completed Successfully Message Screen](image)

**Fig: 3.1.d: Registration Completed Successfully Message Screen**

**Step 4:**

An email confirmation is sent to the provider using the email address provided during registration (see Fig: 3.1.e).

![Welcome Email with Privacy Policy Link after Successful Provider Registration](image)

**Fig: 3.1.e: Welcome Email with Privacy Policy Link after Successful Provider Registration**
3.2 Steps to Register with Validations

3.2.1 Scenario 1: The Provider Enters Incorrect Details.

Step 1:
If you enter incorrect details, you will not be verified and cannot proceed to the next registration step. The “Unable to validate account details provided” error message displays (see Fig 3.2.1.f).

![Fig: 3.2.1.f: User Details not validated during Registration]
Step 2:
The following fields must be entered correctly when you create an account (see Fig: 3.1.c). An error message displays if the following required information is incorrect:

- If “Username” is entered incorrectly.
- If “Email” and “Confirm Email” are invalid and do not match.
- If “Password” is invalid.
- If “Confirm Password” does not match the password entered.
- If “Terms and Conditions” check box is not selected.
- If the same “Security Questions” for question 1 and question2 are selected.
- If the user missed the CAPTCHA values selection.

Example: If “Username” is entered incorrectly.

Fig: 3.2.1.g: Error Message for Entering Invalid Username while Creating Account
Example: If “Email” and “Confirm Email” are invalid and do not match.

Fig: 3.2.1.h: Error Message for Entering Invalid Email Address while Creating Account

Example: If “Password” is invalid.

Fig: 3.2.1.i: Error Message for Entering Invalid Password while Creating Account
Example: If “Confirm Password” does not match the password entered.

![Confirm Password Error Message](image)

*Fig: 3.2.1.j: Error Message for Entering Incorrect Password in Confirm Password Field while Creating Account*

Example: If “Terms and Conditions” check box is not selected.

![Terms and Conditions Error Message](image)

*Fig: 3.2.1.k: Error Message for not selecting the Check Box to Agree to the Terms and Conditions*
Example: If the same “Security Questions” for Security Questions 1 and 2 are selected.

Fig: 3.2.1.1: Error Message for Selecting the Same Security Question during Account Creation
Example: If the user did not select the CAPTCHA.

Fig: 3.2.1.m: Error Message for not selecting the CAPTCHA while Creating User Account when Registering
3.2.2 Scenario 2: If user enters combination of First Name, Last Name and Email Address same as that of an already registered user and tries to register.

![Create Account | Registration](image)

*Fig: 3.2.2.n: Username Reminder Link*
3.2.3 Scenario 3: If user left any/all of the required fields blank.

![Error Message when Fields Left Blank during Registration](image)

3.3 Username Reminder Steps

If you forget your username, click the “Username Reminder” link to request recovery (see Fig: 3.3.p).

![Username Reminder Link](image)
After you click the “Username Reminder” link, the system goes to the “Username Reminder” page where you enter your information (see Fig: 3.3.q).

- Billing NPI Number
- Business Name as it appears on your Explanation of Benefits (EOB)
- Taxpayer Identification Number (TIN)
- First Name
- Last Name
- Email Address you used during registration

*Fig: 3.3.q: Username Reminder Screen*
Click the “Send me a reminder” button and the following message displays (see Fig: 3.3.r).

![Username Reminder Message](image)

**Fig: 3.3.r: Username Reminder Message**

You receive an email that contains your username (see Fig: 3.3.s).

![Email Sent to the Provider for Username Reminder](image)

**Fig: 3.3.s: Email Sent to the Provider for Username Reminder**
4 Provider Secure Log In

The Provider Website has a Secure Log In, where you are asked to enter your Username and Password. This is the same screen you used to set up your online account. If the values match, you are granted access. If the values do not match, an “Invalid Credentials” error message displays (see Fig: 4.a).

![Image of Login Error](image)

*Fig: 4.a: Unable to Login Error – when Provider Tries to Log In with Invalid Credentials*

You are allowed a maximum of 3 failed attempts to log in. More than 3 failed attempts to log in will automatically lock your account, and an error message displays. However, you are given an option to unlock your account (see Fig: 4.b).

![Image of Account Locked Message](image)

*Fig: 4.b: Account Locked Message – when Provider Exceed the Maximum Login Attempts*
4.1 Account Unlock Flow

4.1.1 Scenario 1: Provider is successful in unlocking account by answering only 1 security question.

Step 1:
You can unlock your account by clicking the “Unlock Account” link (see Fig: 4.b). The system goes to the "Unlock Account" page where you enter your User Name to validate your credentials (see Fig: 4.1.1.c). Click the “Continue” button to validate your credentials and go to the next page.

![Unlock Account Screen to Validate Credentials – Provider to Enter Username](image)
Step 2:

You must answer the security question you set during account creation (see Fig: 4.1.1.d). Click the “Continue” button. The system verifies your answer and goes to next page.

![Unlock Account Screen to Validate User – Security Question](image)

Fig: 4.1.1.d: Unlock Account Screen to Validate User – Security Question

Step 3:

After successfully verifying your security answer and identity, the system unlocks your account and you can log in (see Fig: 4.1.1.e).

![Unlock Account](image)

Fig: 4.1.1.e: Provider Account Unlocked Successfully
4.1.2 Scenario 2: If Provider answers the 1st Security Question incorrectly.

Step 1:

Enter your username, which will be validated (see Fig: 4.a). The system goes to Step 2. Enter the answer to your security question.

Step 2:

Enter the answer to the security question you set up during account creation. To verify your identity and go to the next step, click the “Continue” button (see Fig: 4.1.1.b).

Step 3:

If the answer is incorrect, the system goes to next screen and you answer your second security question (see Fig: 4.1.2.f).

Step 4:

After successfully verifying your security answer and identity, the system unlocks your account and you can log in (see Fig: 4.1.2.f).
4.1.3 Scenario 3: If Provider's Username is not verified.

If you enter an invalid username, you are not validated. A “User Not Found” error message displays (see Fig: 4.1.3.g).

![Unlock Account Screen to Validate User – Incorrect Username Entered](image)

4.1.4 Scenario 4: If a Provider is unable to unlock their account by entering invalid security answers for both questions.

If you do not answer your security questions correctly, the system goes to the “Unlock Account” page where you are instructed to send an email to DCALWebMaster@delta.org because your account was not validated (see Fig: 4.1.4.h).

![Unlock Account Screen – Unable to Validate User, Send Email to Unlock Account](image)
4.2 Password Reset Flow

If you want to reset your password, select the “Reset Password” link available on the “Provider Landing” page.

4.2.1 Scenario 1: A Provider successfully resets their password by answering only 1 security question.

Step 1:

If you click the “Reset Password” link, the system goes to the “Reset Password” screen and you enter your User Name to verify your identity (see Fig: 4.2.1.j). Click the “Continue” button to verify your User Name. If the User Name is valid, the system goes to the next page.
Step 2:
Answer the security questions you set up during account creation to verify your identity (see Fig: 4.2.1.k).

Step 3:
After you correctly answer the security question, the system goes to the “Reset Password” page. A message displays stating that an email along with a reset password link has been sent to the email address you provided during registration (see Fig: 4.2.1.l).
Step 4:
You receive an email with a “Reset Password” link (see Fig: 4.2.1.m).

Fig: 4.2.1.m: Reset Password Link in an Email Sent to the Provider
Step 5:

Click the “Reset Password” link to go to the “Reset Password – Token Verification” page to reset your password. Enter your New Password that conforms to the password rules and confirm the New Password (see Fig: 4.2.1.n). Click the “Change Password” button.

The system goes to the “Password has been updated” page (see Fig: 4.2.1.o).
4.2.2 Scenario 2: When Providers successfully reset their password by answering the 2nd security question correctly.

Repeat steps 1 and 2 of Section 4.2.1 (Scenario 1).

If you enter an incorrect answer for the 1st security question, you are prompted to answer the 2nd security question for user identification (See Fig: 4.2.2.p).

If you answer the 2nd security question correctly, the system goes to the “Reset Password” page and informs you to send an email to DCALWebMaster@delta.org to reset your password.

Repeat steps 4 and 5 of Section 4.2.1 (Scenario 1) by clicking the link in the email and updating your password.
4.2.3 Scenario 3: If Providers are unable to reset their password.

If you are unable to answer both your security questions correctly, the system goes to the “Reset Password” page and informs you to email DCALWebMaster@delta.org to reset your password.

![Reset Password – User Unable to Reset Password Screen](image-url)
4.2.4 Scenario 4: When a provider’s password expires

You are required to change your password every 60 days. You cannot reuse your current password or any of the previous 24 used passwords.

If you click on the Login Button after your password is expired, you will be navigated to the Change Password page.

Enter your current password and new password, according to the password rules.

When you click on Change Password Button, you will see the message that your password has been successfully updated and you can click the Log In button in order to login.
4.2.5 Scenario 5: If Provider enters an invalid password.

If you enter a Password that is invalid and does not conform to the password rules, an error message displays (see Fig: 4.2.4.r).

![Fig: 4.2.5.t: Reset Password Error – Password Entered is Invalid](image1)

If the Password and Confirm New Password fields do not match, an error message displays (see Fig: 4.2.4.s).

![Fig: 4.2.5.u: Reset Password Error – Password and Confirm Password do not Match](image2)
If the Password is the same as the current or 24 previous passwords, an error message displays (see Fig: 4.2.4.t).

![Reset password form](image)

Fig: 4.2.5.v: Reset Password Error– Password Should not be the Same as Current or 24 Previous Passwords
5  Denti-Cal Provider Website Tabs

After completing a successful log in, you can access the “Initial Post Login” screen. The available tabs display at the top of the page (See Fig: 5.a).

The “My Practice” tab is the default home page of the provider website. Select the appropriate office location that applies to your inquiry, then click “Apply”.

![Initial Post Login Screen](image)

**Fig: 5.a: Initial Post Login Screen**

5.1  My Practice Tab

The “My Practice” tab displays the most recent activity for that service office, including claims and TAR information associated to any patient for the last 30 days. To select a different provider practice location, click the “Change Location” link to expand the location list (see Fig: 5.1.a).

![Provider Website – My Practice Tab – Change Location](image)

**Fig: 5.1.a: Provider Website – My Practice Tab – Change Location**
Select the appropriate location and click the “Apply” button to view claims specific to the selected location in the list. If you click the “Cancel” button, the location boxes close (see Fig: 5.1.b).

Click the Claim/TAR number (DCN) to get detailed information for a particular Claim/TAR. After you click the DCN, the system goes to a screen that displays specific document details (see Fig: 5.1.c and Fig: 5.1.d).
Another column on the “My Practice” tab under recent activity is “Check/EFT.” This column links the payment record that is associated with a claim. Payment details fall under the category of “Provider Financials.” Click the link for a particular check/EFT. The system displays a screen with a field to enter your Denti-Cal PIN to allow you to access the payment details (see Fig: 5.1.e).
If you do not enter the correct Denti-Cal PIN and click the “Continue” button, the following error message displays (see Fig: 5.1.f).

![Fig: 5.1.f: Provider Website – My Practice Tab – Check/EFT – PIN not Valid Screen](image-url)
5.2 Claim/TAR Tab

Click the “Claim/TAR” tab to view Your Claims and TARs for the past two years. You can change the service office location you want to inquire on by selecting “Change Location”.

You can search based on either the Patient’s Name or Claim/TAR number, along with the pull-down option list to view claims from the Last 30 days, Last 60 days, Last 90 days or all the claims for the patient name or claim/TAR number selected (see Fig 5.2.g). You can also conduct a wild card search. (Example: Instead of entering the entire TAR# /Patient Name you can even enter the first two numbers of the TAR# or any alphabets from the Patient Name in the Search by # or name field).

All the search filters work independently.

![ Provider Website – Claim/TAR Tab with search filters highlighted ]

Fig: 5.2.g: Provider Website – Claim/TAR Tab

Similar to the “My Practice” tab, you can click an individual claim/TAR # to display its corresponding details. After you click the Check/EFT # link, the system prompts you to enter your Denti-Cal PIN. This link is not accessible unless you enter the correct Denti-Cal PIN.
5.3 Payments

To check your financial information, click the “Payments” tab and enter the Denti-Cal PIN that is specific to your office location (see Fig: 5.3.1.h).

5.3.1 Scenario 1: When provider enters correct PIN.

After you enter the PIN correctly, the system goes to the “Payment History” screen and you can view your payment history (see Fig: 5.3.1.i).
Similar to the “My Practice” and “Claims” tabs, you can view your Check/EFT by clicking the applicable Check/EFT # link in the Check/EFT # column (see Fig: 5.3.2.j).

5.3.2 Scenario 2: When provider enters an incorrect PIN.

If you enter an incorrect PIN, you cannot view your payment history and the “PIN is not valid” message displays (see Fig: 5.3.2.k).
5.4 Account Tab

You can view and edit/update your personal information like Email Address, First Name, Last Name, Password and Security Questions.

5.4.1 Scenario 1: If a Provider is an Administrator (Admin).

The Denti-Cal Provider Website’s administrator has different rights than regular users. Admin providers can view and update the details of other users through the “Manage Users” tab (see Fig: 5.4.1.i).

![Fig: 5.4.1.i: Provider Website – Account Tab – Admin User]
5.4.2 Scenario 2: When a provider is a Regular User.

Regular Users cannot view the “Manage Users” tab. They can only update/view their own details (see Fig: 5.4.2.m).

Fig: 5.4.2.m: Provider Website – Account Tab – Regular User
5.4.3 Scenario 3: Successfully changing Password from the Accounts Page.

To update your password, click the “Change Password” button on the “Accounts” tab. The section to update the password expands and you can successfully change your password (see Fig: 5.4.3.n and Fig: 5.4.3.o).

![Provider Website – Account Tab – Change Password Button](image-url)
5.4.4 Scenario 4: When a Provider successfully updates their password – Account tab.

Click the “Change Password” button to expand the section and update your password. Update the “Current Password,” “New Password,” and “Confirm Password” fields based on the password rules.

After you click the “Update Profile” button, the “User Profile Updated Successfully” message displays and the update password section closes.
5.4.5 Scenario 5: When a Provider is unable to update their password through the Account tab.

You can update your password from the “Account” tab. However, this process fails if it is not performed correctly.

If you enter a new password that is the same as the current password, an error message displays (see Fig: 5.4.4.q).
If you enter any of the 24 previously used passwords, an error message displays (see Fig: 5.4.4.r).

If the New Password and Confirm Password do not match, an error message displays (see Fig: 5.4.4.s).

If the New Password does not conform to the password rules, the following message displays (see Fig: 5.4.4.t).
6 Admin Functionality Features

6.1 Manage Users

Providers who are administrators (admin) of the Denti-Cal Provider Website can only view the “Manage Users” tab from the “Accounts” tab (see Fig: 6.1.a).

An admin provider clicks the “Manage Users” link to display the “Add User” button and a list of users (providers) of the website along with their details like First Name, Last Name, Email, Username and Registered type. Admins can edit user information, delete their records or “Re-Send Invite” to unregistered providers (see Fig: 6.1.b).
6.1.1 Add User

A Provider with admin rights clicks the “Add User” button to add users. After you click the “Add User” button, the system goes to the “Add User” page. Enter provider details like First Name, Last Name, Email Address and User Type (see Fig: 6.1.1.c).

After entering the correct details, click the “Invite” button to send an email with a registration link to the provider (see Fig: 6.1.1.d).

Fig: 6.1.1.c: Provider Website – Add User Page

Dear xxx

You have been successfully added to our provider portal. Please use the following link to complete your registration.

Registration Link

California Medi-Cal Dental Program, P.O. BOX 15539, Sacramento, CA 95852-1539 | Denti-Cal Privacy Policy

Fig: 6.1.1.d: Provider Website – Email Sent to the added User with a Registration Link
When a newly added provider clicks the “Registration Link,” the system goes to Registration Page 1. Validate the details by correctly entering the Email, First Name and Last Name. To go to the next registration step, click the “Validate” button (see Fig: 6.1.1.e). After registering, the registered type from the user list updates from “N” to “Y.”

Registration Page 2 is same as the registration process (see Fig: 3.1.c).
6.1.1.1 Scenario 1: If Provider enters details with same combination of First Name, Last Name and Email of an already added user.

If you enter the First Name, Last Name and Email address (using the same combination) of an already registered user, an error message “User already exists” displays. (See Fig: 6.1.1.1.f)

![Fig: 6.1.1.1.f: Provider Website – User already exists while adding user](image-url)
6.1.1.2 Scenario 2: If Provider enters invalid details.

If you enter an invalid Email address or do not select the correct User Type, an error message displays and the invalid fields are highlighted (see Fig: 6.1.1.2.g).

![Fig: 6.1.1.2.g: Provider Website – Invalid Details Entered while Adding User](image)

If an added user tries to register with invalid details by using the “Registration Link” from the email, the user is not validated and will be unable to register. The “Invalid Details Entered” error message displays (see Fig: 6.1.1.2.h).

![Fig: 6.1.1.2.h: Registration Page 1](image)
6.1.1.3 When an added user tries to register.

After the provider is validated in the previous step, the system goes to Step 2 of the registration process. The First Name, Last Name and Email fields auto populate along with the Business Name, NPI and TIN number (see Fig: 6.1.1.3.i).

All other fields are the same as the normal registration. An error message displays if you try to register with a username that is already in use. (See Fig: 6.1.1.3.j)
6.1.2 Edit Users

Administrators click the “Edit” button to edit details of any user from the user list (see Fig: 6.1.2.k).

Click the “Edit” button to go to the “Edit User” page where administrators can edit/update provider details like Email address and User Type (see Fig: 6.1.2.l).
6.1.2.1 Scenario 1: If provider enters invalid details.

If you enter an incorrect Email address, an error message displays. The field is highlighted and you cannot update the details (see Fig: 6.1.2.1.m).

![Fig: 6.1.2.1.m: Provider Website – Edit User Page, Invalid Details Entered](image)

6.1.3 Delete Users

Administrators click the “Delete” button to delete details of any user from the user list (see Fig: 6.1.3.n).

![Fig: 6.1.3.n: Provider Website – Delete Button from User List](image)

A “Confirmation” message displays. Click the “Confirm Delete” button to confirm the deletion (see Fig: 6.1.3.o).
After you click the “Confirm Delete” button, the user is removed from the list and the list is updated (see Fig: 6.1.3.p).
7 Reporting a Missed Appointment Feature

You can report any missed beneficiary appointments to Denti-Cal Staff through a link available on your “My Practice” page (see Fig: 7.a).

Click the “Report a missed appointment” link to go the “Missed Appointment Notification” form page. Some provider details auto populate; however, auto populated information can be changed, if needed. Complete the Beneficiary Information correctly. Indicate if the beneficiary has missed any prior appointments and select the verification statement. Click the “Send” button to submit the form (see Fig: 7.b).
Fig: 7.b: Provider Website – Missed Appointment Link on the My Practice Page
Click the “Send” button to trigger an email (see Fig: 7.c).

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Billing NPI Number</td>
<td>xxx</td>
</tr>
<tr>
<td>Service Office Number</td>
<td>001</td>
</tr>
<tr>
<td>Contact Phone Number</td>
<td>xxx</td>
</tr>
<tr>
<td>Contact Person</td>
<td></td>
</tr>
<tr>
<td>Contact Email</td>
<td>xxx</td>
</tr>
<tr>
<td>Provider License Number</td>
<td></td>
</tr>
<tr>
<td>Beneficiary Last Name</td>
<td>xxx</td>
</tr>
<tr>
<td>Beneficiary First Name</td>
<td>xxx</td>
</tr>
<tr>
<td>Medi-Cal ID Number</td>
<td>xxx</td>
</tr>
<tr>
<td>Date of Birth</td>
<td></td>
</tr>
<tr>
<td>Beneficiary Representative</td>
<td>xxx</td>
</tr>
<tr>
<td>Address</td>
<td>xxx</td>
</tr>
<tr>
<td>City</td>
<td>DURHAM</td>
</tr>
<tr>
<td>State</td>
<td>CA</td>
</tr>
<tr>
<td>Zip code</td>
<td>75062</td>
</tr>
<tr>
<td>Phone Number</td>
<td>xxx</td>
</tr>
<tr>
<td>Alternative Phone Number</td>
<td>xxx</td>
</tr>
<tr>
<td>Appointment Date</td>
<td>06/12/2017</td>
</tr>
<tr>
<td>Appointment Time</td>
<td>09:00 AM</td>
</tr>
<tr>
<td>Prior Appointments</td>
<td>Yes</td>
</tr>
<tr>
<td>Missed Visits</td>
<td>11</td>
</tr>
<tr>
<td>Notes</td>
<td>aaaaaaa</td>
</tr>
</tbody>
</table>

*Fig: 7.c: Provider Website – Missed Appointment Link on the My Practice Page*

### 7.1 Scenario 1: If Provider enters invalid details in the Missed Appointment Form.

The fields with a red asterisk (*) are mandatory fields. If you do not enter the details in these fields, an error message displays (see Fig: 7.1.d).

*Fig: 7.1.d: Provider Website – Missed Appointment Form – Details not Entered Error*
If you enter details that do not match the field’s format, an error message displays (see Fig: 7.1.e).

![Fig: 7.1.e: Provider Website – Missed Appointment Form – Invalid Details Entered]

8  Provider Resources

You can access Denti-Cal site links from your secure area. This list of external links are available in the Provider Resources section of the "My Practice" tab (see Fig: 8.a).

![Fig: 8.a: Provider Website – Provider Resources – Links on the My Practice Tab]
9 Contact Us Page

Denti-Cal providers can view the ‘Contact Us’ page for getting Denti-Cal’s toll free number or any reference email addresses.

Fig: 9.a: Provider Website – Contact Us Page

Reference List:

- **Provider Toll Free Line**: 1-800-423-0507
- **For questions, comments or feedback** about the program contact: [DCALInfo@delta.org](mailto:DCALInfo@delta.org)
- **To report any website technical problems or issues** contact: [DCALWebMaster@delta.org](mailto:DCALWebMaster@delta.org)