



2019

Short-Doyle Medi-Cal (SDMC)

User Manual

An instructional guide for **Counties & Direct Providers** who submit medical claim data to the **Department of Health Care Services**

Revision History

Version Number	Date Created	Description
1.0	08/08/2019	First iteration of working rough draft
1.1	08/19/2019	Changed Approver certification form location on DHCS internet
1.2	08/29/2019	Added SDMC-DMH Approver ownership to include the MMEF system

Table of Contents

I. Introduction	4
A. <u>Purpose</u>	4
II. Short-Doyle Medi-Cal (SDMC) System Access	4
B. <u>Certifying New County Approvers</u>	4
(a) Where to obtain the new SDMC Approver Certification Forms	4
C. <u>Accessing the DHCS Application Portal</u>	5
(a) Logging in using Azure Active Directory (AAD)	5
D. <u>Enrolling New SDMC Users</u>	6
(a) An Approvers Rights & Responsibilities as a Security Group Owner	6
(b) Department of Mental Health (DMH)	6
(c) Alcohol & Drug Program (ADP)	7
E. <u>Completing Access Reviews</u>	7
(a) A security measure to restrict access to only those who need it	8
III. SDMC Graphical User Interface	9
F. <u>Accessing the SDMC Web Application</u>	9
(a) Logging into Production or Test Environment	9
(b) Opening MoveIT File Transfer from SDMC Website	10
G. <u>Checking a Submitted File's Processing Status</u>	11
(a) How to Filter Claim Data presented to User	11
H. <u>Enrolling into Electronic Funds Transfer (EFT)</u>	12
(a) How to Enroll into the EFT Service	13
(b) Testing Enrollment in the Staging Environment	14
(c) Changing or Cancelling an Enrollment	15
(d) EFT Enrollment Process Overview	16
IV. MoveIT File Transfer GUI	17
I. <u>Accessing the MoveIT File Transfer Service</u>	17
(a) Logging into MoveIT	18
(b) Uploading Data Files to MoveIT	18
(c) Downloading SNIP Reports (SR), 999s, 835s, and Transmission Acknowledgements (TA1)	18
(d) Submitting Test Files to the Staging Environment	18
(e) System Notifications	18
V. Contacting SDMC Support	19
J. <u>Opening a Remedy Request Ticket</u>	19

Introduction

A) Purpose

The information contained within this document helps explain the process for all **Counties** and **Direct Providers** who submit medical claims data to the **Department of Health Care Services (DHCS)**. In it you will find the necessary steps to procure new **Approvers** for the **Short-Doyle Medi-Cal (SDMC)** system, including both the **Department of Mental Health (DMH)** and the **Alcohol & Drug Program (ADP)**; How Approvers can add/remove new **SDMC Users** for their organization; How to login and use the new **SDCM Graphical User Interface (GUI)**, and enroll for **Electronic Funds Transfer (EFT)**; How to use the **MoveIT File Transfer GUI** for uploading/downloading files; and lastly how to contact **SDMC Production Support** for any of your technical needs.

Short-Doyle Medi-Cal (SDMC) System Access

B) Certifying New County Approvers

To ensure the confidentiality of patient mental health or drug Medi-Cal data, **DHCS** requests that the County Mental Health Director, AOD Administrator, or Direct Provider's Executive Officer designate just two contacts to be responsible for approving county staff requests to upload or access confidential patient data in the **SDMC** system. **Approver Certification** forms can be located on the [DHCS](#) website under [Mental Health Forms](#). Completed certification forms should be signed by all parties involved, and emailed to MEDCCC@dhcs.ca.gov for both **DMH** and **ADP**. All instructions are included on the form. If you've any questions, please contact ITServiceDesk@dhcs.ca.gov for support. (See figure B1)



BHIS Certification Forms

[DHCS 5259 \(06/16\): CSI County Approver Certification & Vendor Appointment Form](#)

[DHCS 5262 \(Rev. 07/17\): DCR County Approver Certification and Vendor Appointment Form](#)

[DHCS 5260 \(Rev. 06/18\): FAST County Approver Certification & Vendor Appointment Form](#)

[DHCS 5267 \(10/18\): Provider Information Management System \(PIMS\) County Approver Certification & Vendor Appointment Form](#)

ITWS Certification Forms

[MC 5254: ITWS Business Partner Certification](#)

[MC 5257: ITWS DHCS Employee Certification](#)

[MC 5258: ITWS Vendor Certification](#)

[MC 5273: ITWS County Certification](#)

Figure B1: DHCS Website Page for Program Forms

C) Accessing the DHCS Application Portal

After a new approver has been vetted by the designated **DHCS** program office, their request will be routed through **SDMC Production Support** to the **Cloud Team**. There they will be added to the **Azure Active Directory (AAD)** as a **Security Group Owner** for their county's/direct provider's **SDMC Security Group**. Once an **AAD** user account has been created for the approver, they'll be notified by email that they can now login to the [DHCS Application Portal](#). (See figure C1)

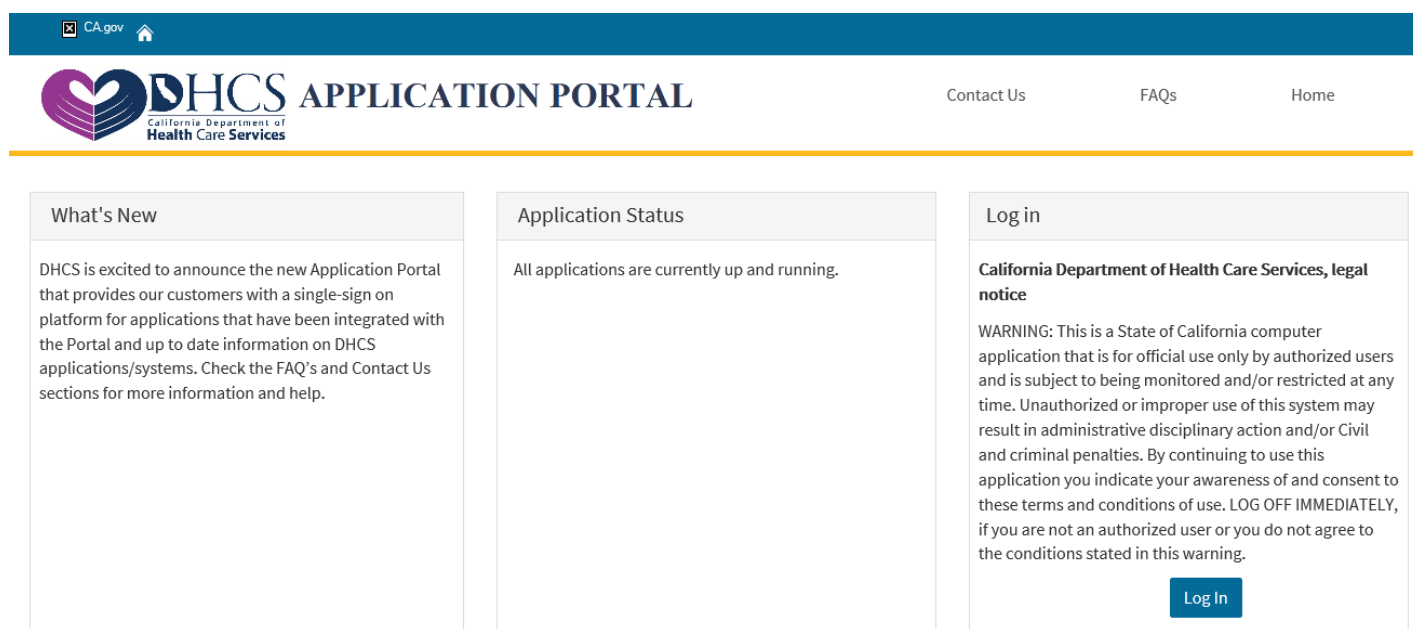


Figure C1: DHCS Application Portal

NOTE: When logging into the **DHCS Application Portal** for the first time, you may be requested to set up **Two-Factor Authentication (2FA)**

D) Enrolling New SDMC Users

Once an **Approver** has been made the **SDMC Security Group Owner** for their organization, they will have the ability to **Add** or **Remove** staff members for that system. To do this, **Approvers** will click on the **Groups** icon listed on the **Apps** screen. (See figure D1)

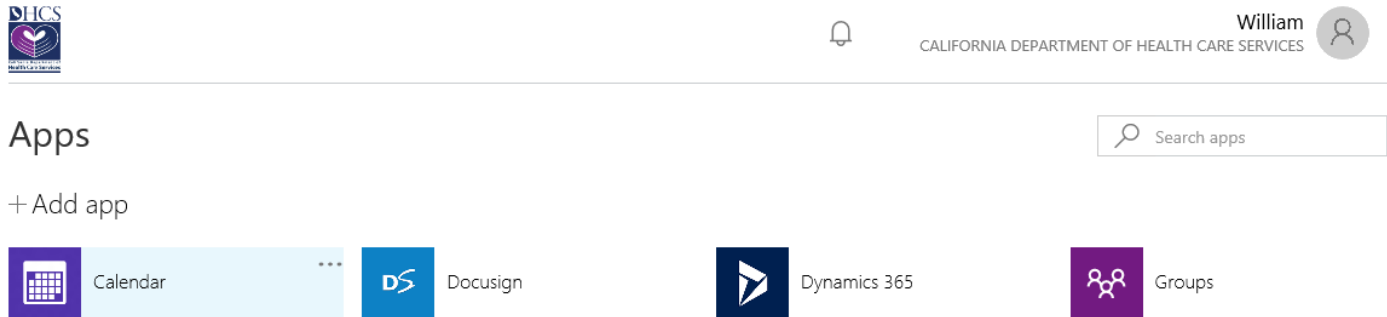


Figure D1: Azure AD Application for adding/removing members to Groups

The **Groups** screen will show an **Approver** both the groups they are in, and the groups they are owners of. An **SDMC-DMH Approver** for *county/direct provider* will be granted ownership of both **AZ-SDMC-[county/direct provider]-DMHAnalyst**, and **AZ-SDMC-[county/direct provider]-MMEFAnalyst**. An **SDMC-ADP Approver** for *county/direct provider* will be granted ownership of **AZ-SDMC-[county/direct provider]-ADPAnalyst**. Clicking on an owned group will take you to the **Groups Members** screen. (See figure D2)

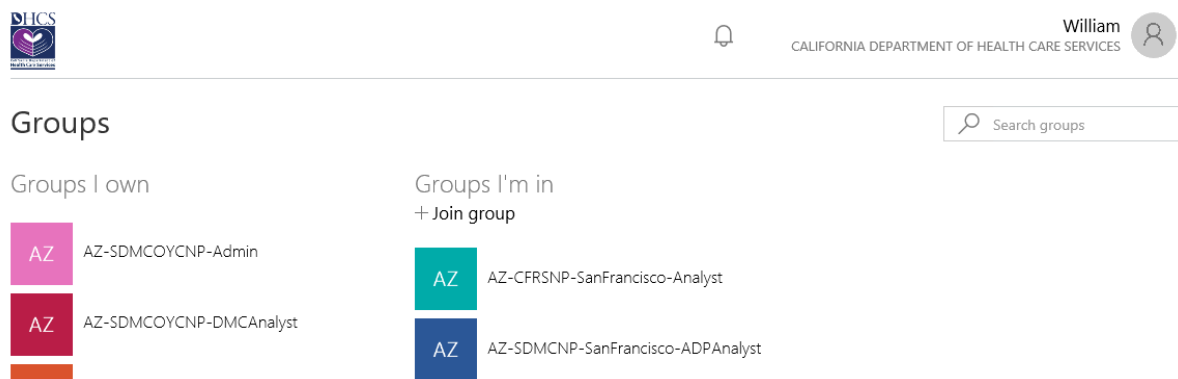


Figure D2: Azure Active Directory Groups Screen

The primary function of the **Group's Members** screen is for the assigned **Approvers** to **Add** or **Remove** staff member access for the county/direct provider they reside over. (See figure D3)

← Groups



AZ-SDMCOYCNP-Admin

SDMC OOYC / 911 Non-Prod Security Group for Permission Access

Group type: Security

Members: 8

Join policy: Only the owner of this group can add members

[Edit details](#) [Delete group](#)








MEMBERS	ROLE	ID	+
 Butt, Zaibunnisa...	Owner	Zaibunnisa.Butt@dhcs.ca.gov	
 Chandra Sekara...	Member	Jeeva.ChandraSekaran@dhcs...	...
 Davis, Chris (EITS...	Owner	Chris.Davis@dhcs.ca.gov	
 Jilakara, Yagnara...	Member	Yagnaraja.Jilakara@dhcs.ca.g...	...

Figure D3: Azure Active Directory Groups Members Screen

CAUTION: Editing details or Deleting groups is strictly **prohibited**, and use of these functions can result in having your **Ownership revoked!**

To **Add** a member select the **plus (+)** symbol shown above the member list. To **Remove** a member select the **ellipsis (...)** shown next to the member's name, then select **Remove member**. (See figure D4)

MEMBERS	ROLE	ID	+
 Butt, Zaibunnisa...	Owner	Zaibunnisa.Butt@dhcs.ca.gov	
 Chandra Sekara...	Member	Jeeva.ChandraSekaran@dhcs...	...
 Davis, Chris (EITS...	Owner	Chris.Davis@dhcs.ca.gov	

Remove member

Figure D4: Azure Active Directory Member functions for adding/removing staff members

NOTE: A new member can be added only when the member's **Email Domain** has been approved and whitelisted by DHCS.

E) Completing Access Reviews

Periodically, **Security Group Owners** are responsible for completing **Access Reviews** in order to ensure that the system users who were made members of their organization's **Security Group** continue to need that access. Around once every 3 to 6 months, **SDMC Approvers** will receive a **Microsoft Azure AD Notification Service** email requesting them to review the listed members' access for their **Security Group**. Simply click the **Start Review** link to begin the process. An **Approver** can also open **Access Reviews** from their **Apps** page by clicking on the app itself. (See figure E1)

Apps

+ Add app



Calendar



Docusign



Dynamics 365



Groups



File Transfer Test



Flow




Forms



Access reviews

Figure E1: Azure AD Application for reviewing access to a Security Group

NOTE: if the **Access Reviews** tile  isn't visible, then no action is required, as there are no reviews to perform at that time.

All **Access Review** requests must be completed in a timely manner. Otherwise, **Security Group** members may be removed, thus causing them to be unable to access the **DHCS Application** associated with that **Security Group**.

For further details on any of the **Security Group Owner** rights, features, or functionality, please refer to the [Security Group Owner's Manual](#) located on the [DHCS Application Portal](#) login page under **User Guides**.

SDMC Graphical User Interface

F) Accessing the SDMC Web Application

The **DHCS Application Portal** leverages **Microsoft's Azure Management Portal** by enabling someone with a **Microsoft Office 365 (O365)** account (*also referred to as **Azure Active Directory (AAD)** or **O365 AAD***) for providing access to all **DHCS Applications**. Users who've been granted membership by their organization's Approvers can login to the Portal using their credentials for an existing **O365 AAD** or **Microsoft** account; provided that it was established using their organizations email domain, and that domain was whitelisted by DHCS. If a user does not have either type of accounts, then they'll be asked to create one when attempting to log into the **DHCS Application Portal** for the first time. This process may differ slightly depending on the type of account or web browser being used. For further details please refer to the [DHCS Application Portal User's Manual](#).

When an **SDMC Approver** adds a staff member to their organizations **SDMC Security Group**, that user should receive a **Microsoft Azure** email telling them to "**Let's Get Started**". Once a user has logged into the Portal, they'll be taken to their personal **Apps** page listing all of the applications they have access to. **Short-Doyle Medi-Cal Users** who've been granted membership to either **SDMC-DMH** or **SDMC-ADP** should see application icons for both **SDMC Production** and **SDMC Test**. (See figure F1)

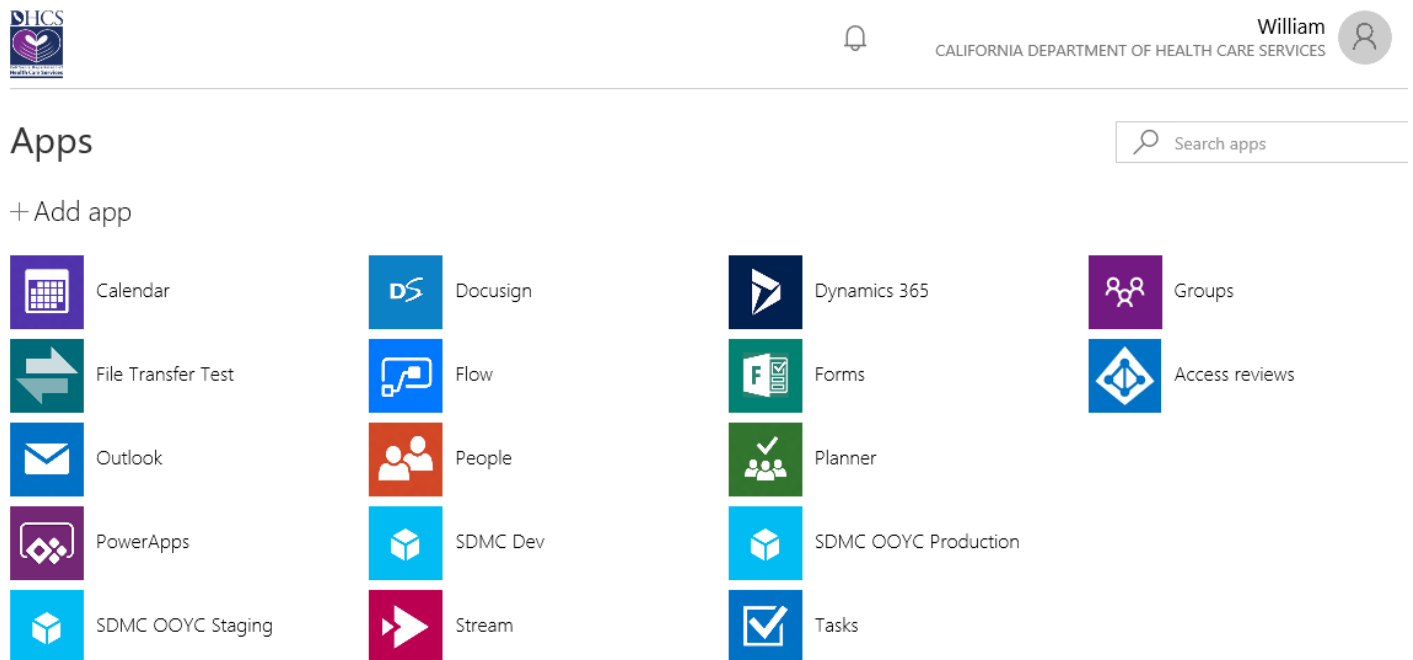


Figure F1: Azure AD Apps page listing the icons for SDMC Production & SDMC Test

NOTE: When logging into the **SDMC Application** for the first time, if you’ve not already done so, then you may be requested once again to set up **Two-Factor Authentication (2FA)**

Clicking on an **SDMC Application** icon will automatically open that environment in a new web browser tab. The **SDMC Test** environment can be used by staff members in order to test a medical claim data file to ensure that the files your organization is submitting meet all **HIPAA** standards. However, a county/direct provider should never submit official medical data to **SDMC Test** for maintaining the security of confidential **Patient Health Information (PHI)**. A message will scroll across the screen to show you which environment you’re currently working in. (See figure F2)

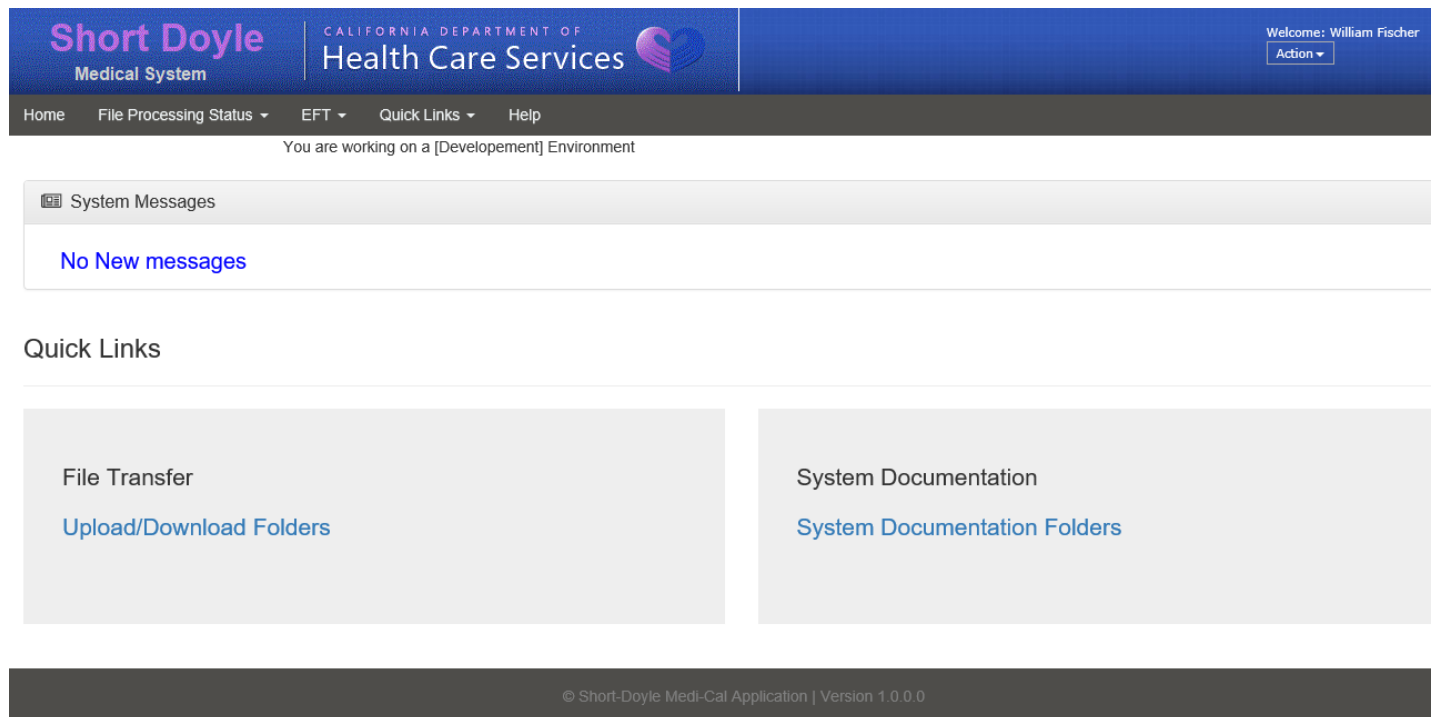


Figure F2: SDMC Web Application Graphical User Interface (GUI)

NOTE: The **MoveIT File Transfer** can be accessed through the **SDMC GUI** by clicking on the **Quick Link**

G) Checking a Submitted File's Processing Status

A submitted claim's processing status can be determined by selecting one of the specified file types listed under the **File Processing Status** dropdown list. (See figure F3)

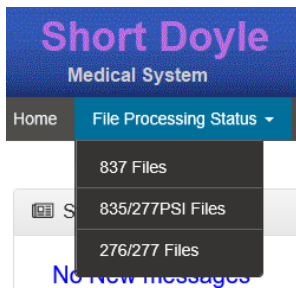


Figure F3: Accessing a Data File's Processing Status

Selecting a particular file type will open the **Details View** for those kind of data files. There you will be able to **Search** for a specific filename, or **Filter** data by **Program (DMH or ADP)**, **County**, or within a specified time period. The records panel can display up to **500** records spread over multiple pages, and the table containing the data can also be used to sort information by clicking on the column headers. (See figure F4)

The screenshot displays the 'Short Doyle Medical System' header with the 'CALIFORNIA DEPARTMENT OF Health Care Services' logo. A user greeting 'Welcome: William Fischer' is visible. The navigation bar includes 'Home', 'File Processing Status', 'EFT', 'Quick Links', and 'Help'. A status message indicates 'You are working on a [Development] Environment'. Below the navigation bar is a 'Search Filter' section with fields for 'File name', 'Program' (set to 'DMH'), 'County' (set to 'SAN FRANCISCO-38'), 'From Date', and 'To Date'. A 'Search' button is present. The main content area is titled '837 Details' and contains a table with 10 columns: 'Input File Name', 'Uploaded Date', 'Status', 'User Uploaded', '999 Count', 'TA1', 'Uploaded Date', 'SR Report', 'Uploaded Date', and 'County'. The table displays 10 rows of data, all with a status of 'Accepted'. At the bottom, there is a pagination control showing 'Page 1 of 5' and a 'View 1 - 10 of 50' option.

Figure F4: Details View for Claim Processing Status

The **Status** shown for submitted **837** data files only verifies certain elements pertaining to the filename convention, file types, associated county or program, but whether or not the data contained within the file is valid still needs to be determined by the county/direct provider using the information returned in the **Snip Report (SR)**, **999**, and **Transmission Acknowledgement (TA1)**.

NOTE: The submitted **.zip** files should no longer be **encrypted** with **password** protection

H) Enrolling into Electronic Funds Transfer (EFT)

The **EFT** process provides **Trading Partners (TP)** with the option to receive **electronic payments** for submitted claims as opposed to **paper warrants**. Section **1104** of the **Affordable Care Act (ACA)** mandates health plans to support **EFT** transactions as a standard of the **Health Insurance Portability Accountability Act**. **TPs** who submit **837** claims files through the secure **MoveIT File Transfer** to be adjudicated by **Short-Doyle Medi-Cal (SDMC)**, and are not enrolled for **EFT**, will continue to receive a **paper warrant** and an **835 Electronic Remittance Advice (ERA)** from the **SDMC** system. Participation in the **EFT Enrollment Process** is not a mandatory requirement.

To participate in the **EFT Enrollment Process**, each **TP** is required to register two **Approvers** as **Security Group Owners** for the **SDMC Graphical User Interface (GUI)**. This will allow the **Approvers** to add new members for their organization to the **SDMC Security Group** which in turn grants those **Users** access to the **SDMC** application. Once access has been granted, a **User** will be able to select **EFT Enrollment** from the **EFT** dropdown list. (See figure H1)

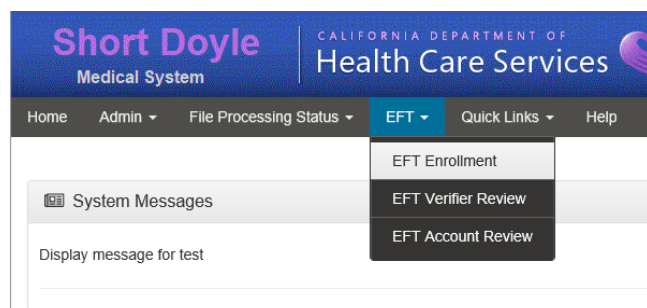


Figure H1: SDMC GUI Dropdown List for EFT Enrollment

On the **EFT Enrollment** screen, the **User** will be able to see all previous submissions for all the organizations they belong to in the **EFT Details** table view. To enter a new **EFT Enrollment Form**, the **User** simply clicks on the **Add** button located at the upper right side of the panel. (See figure H2)

The screenshot shows the 'Short Doyle Medical System' header with the 'CALIFORNIA DEPARTMENT OF Health Care Services' logo. A navigation bar includes 'Home', 'File Processing Status', 'EFT', 'Quick Links', and 'Help'. A message states 'You are working on a [Development] Environment'. The main content area is titled 'EFT Enrollment' and contains a sub-section 'EFT Details' with an 'Add' button. Below this is a table with columns: Provider Name, TIN, NPI, ContactName, Status, CreatedBy, and CreatedDate. The table is empty, showing 'Page 1 of 0' and 'No records'.

Figure H2: EFT Enrollment Screen listing all previous Enrollment Details

The **EFT Enrollment Form** must be completed twice: first in the **Test** environment (**Staging**), and once again in the **Production** environment. (See figure H3)

The screenshot shows the 'EFT Enrollment: Add EFT provider Details' form. It is divided into several sections: 'Provider Information' (Provider Name *, Doing Business As, Street Address *, City *, State *, Zip *), 'Provider Identifiers Information' (TIN/EIN *, National Provider Identifier NPI *, Assigning Authority *, Trading Partner *, Program), 'Provider Contact Information' (Provider Contact Name *, Contact Title *, Contact Telephone # *, Telephone # Ext., Contact Email Address, Contact Fax Number), and 'Provider Agent Information' (Provider Agent Name, Agent Street Address, Agent City, Agent State, Agent Zip, Agent Contact Name, Agent Contact Title, Agent Telephone #, Agent Telephone # Ext., Agent Email Address, Agent Fax Number). Required fields are marked with a red asterisk. At the bottom are 'Next' and 'Reset' buttons.

Figure H3: EFT Enrollment Form

NOTE: Any required fields are highlighted with a red asterisk *

Prior to completing **EFT Enrollment** in the **Production** environment, **TPs** must test their systems. To test the **EFT** system changes, **TPs** are instructed to submit non-official **837** claims files for testing in the **Staging** environment using de-identified **Patient Health Information (PHI)** data. A **Remedy** request ticket will be created by the **Program Verifier** to track progress during testing. All email communications between DHCS and the TP during testing must reference the ticket number provided by DHCS.

Participants in the **EFT Process** will notice changes in the **835 ERA** transactions, including the newly added **Trace Number** as opposed to the customary **Warrant Number**. EFT offers a consistent and uniform way for TP's to reconcile the EFT payment and the 835 ERA, and will help to improve the following:

- Alleviate posting delays
- Increase the ability to conduct targeted follow-up with health plans and/or patients
- Provide accurate and efficient payment of claims

TPs must report all banking changes by completing another **EFT Enrollment Form** in the **Production** environment. Changes to the **bank selection**, **routing number**, or **account number** will revert the **TP** back to **paper warrant mode** while the **EFT** changes are being processed. This process can take up to **60 calendar days** to finalize the **EFT** bank changes. (See figure H4)

EFT Enrollment: Add EFT Financial Details

Back

Financial Institute Information

Institute Name *

Street Address *

City *

State *

Zip *

Telephone # *

Telephone # Ext.

Routing Number *

Account Type *

Account Number *

Provider TIN *

Provider NPI *

Bank Letter

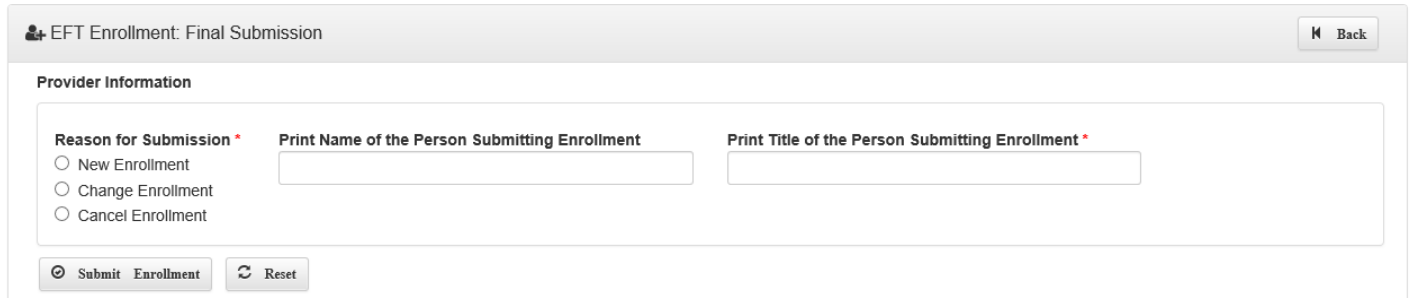
Browse...

Next

Reset

Figure H4: EFT Enrollment Form Financial Details

All other EFT changes will not revert the TP to paper warrant mode. To avoid any delay in payment, please do not close your old banking account until your new account is activated and receiving payments. If the TP elects to cancel EFT participation, the TP must complete the EFT Enrollment Form and select Cancel Enrollment under the section for Final Submission. Please allow up to 60 calendar days for DHCS to finalize the EFT cancellation and reinstate the TP back to paper warrants. (See figure H5)



The screenshot shows a web form titled "EFT Enrollment: Final Submission". At the top right is a "Back" button. Below the title is a section labeled "Provider Information". Inside this section, there are three fields: "Reason for Submission *" with three radio button options ("New Enrollment", "Change Enrollment", "Cancel Enrollment"), "Print Name of the Person Submitting Enrollment" with a text input field, and "Print Title of the Person Submitting Enrollment *" with a text input field. At the bottom of the form are two buttons: "Submit Enrollment" and "Reset".

Provider Information		
Reason for Submission * <input type="radio"/> New Enrollment <input type="radio"/> Change Enrollment <input type="radio"/> Cancel Enrollment	Print Name of the Person Submitting Enrollment <input type="text"/>	Print Title of the Person Submitting Enrollment * <input type="text"/>
<input type="button" value="Submit Enrollment"/> <input type="button" value="Reset"/>		

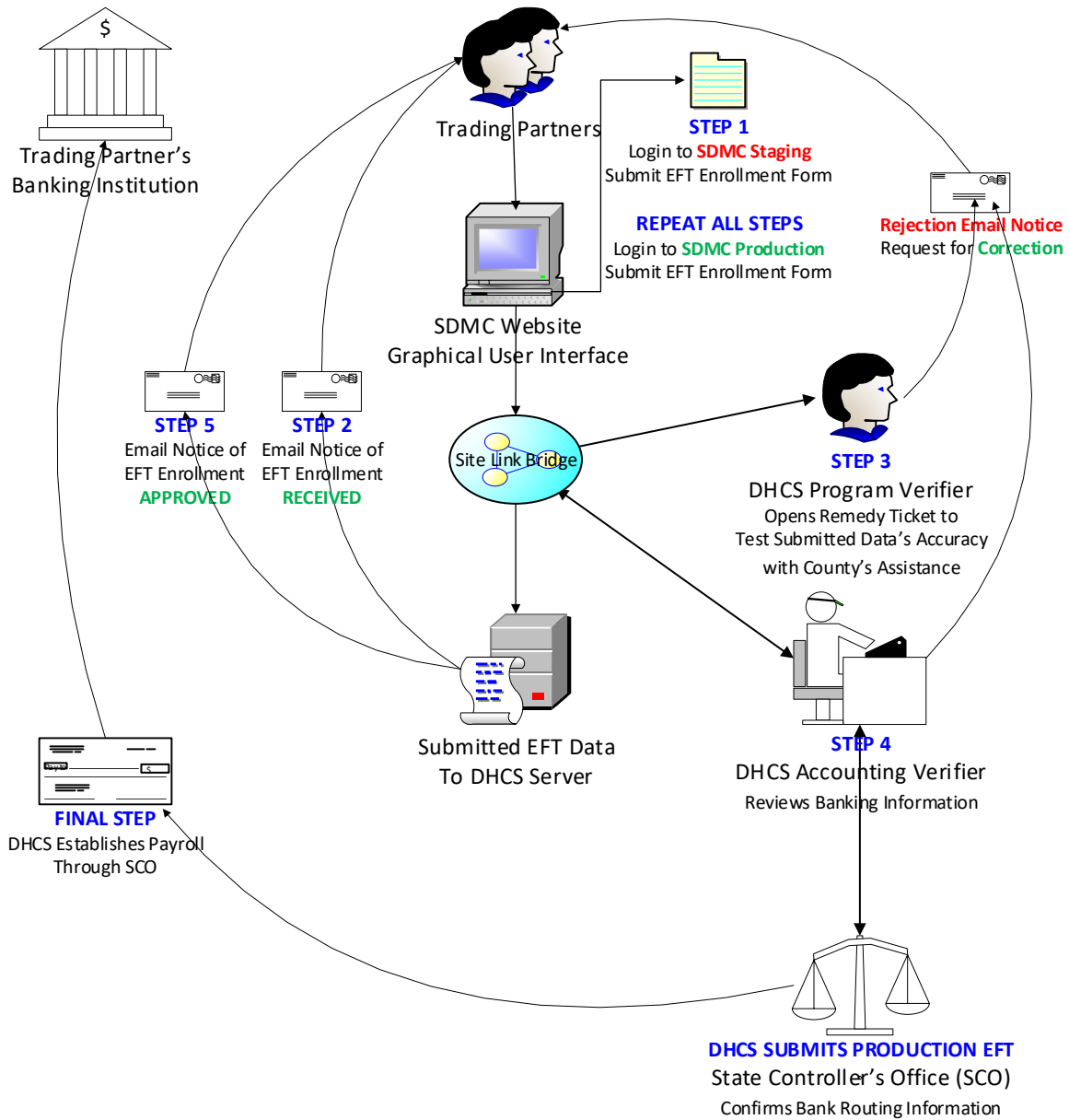
Figure H5: EFT Enrollment Form Final Submission

Department of Healthcare Services

High-Level Overview

For


The Electronic Funds Transfer Enrollment Process



MoveIT File Transfer GUI

I) Accessing the MoveIT File Transfer Service

SDMC Users will now upload/download claims data files through the **MoveIT File Transfer Service**.

To log into the **File Transfer Service** from the [DHCS Application Portal](#), simply click on the **File Transfer** application icon  shown on your personal **Apps** page. (See figure I1)

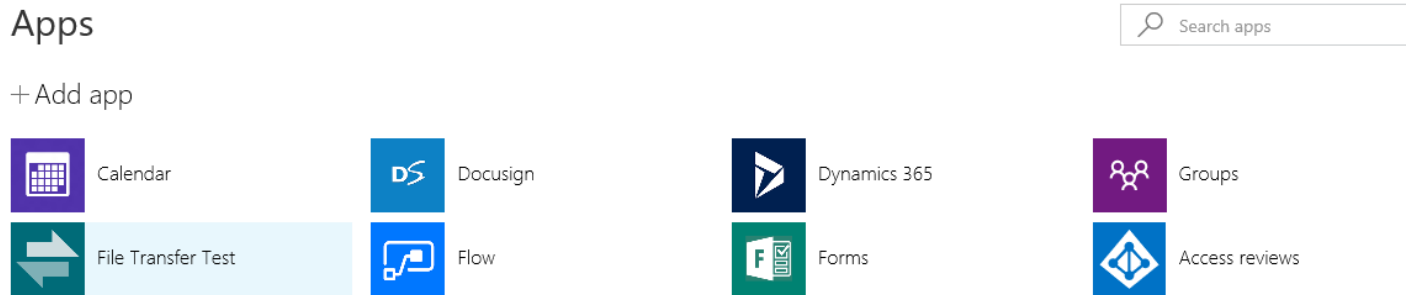


Figure I1: Azure AD Apps page showing icon for MoveIT File Transfer Service

NOTE: The **MoveIT File Transfer** can also be accessed through the **SDMC GUI** by clicking on the **Quick Link**

Opening the **File Transfer Service** from the **Apps Portal** will take you directly to the **MoveIT Home Page**. From there, you'll need to navigate to **FOLDERS\BHIS** where you'll have the option to open either the **Production** or **Staging** environments. As mentioned previously, the **Staging** environment is for the purpose of conducting **User Acceptance Testing (UAT)** and **Quality Assurance (QA)** so **Trading Partners (TP)** can submit test files in order to ensure that the data submitted is meeting all **HIPAA** format standards. (See figures I2 & I3)

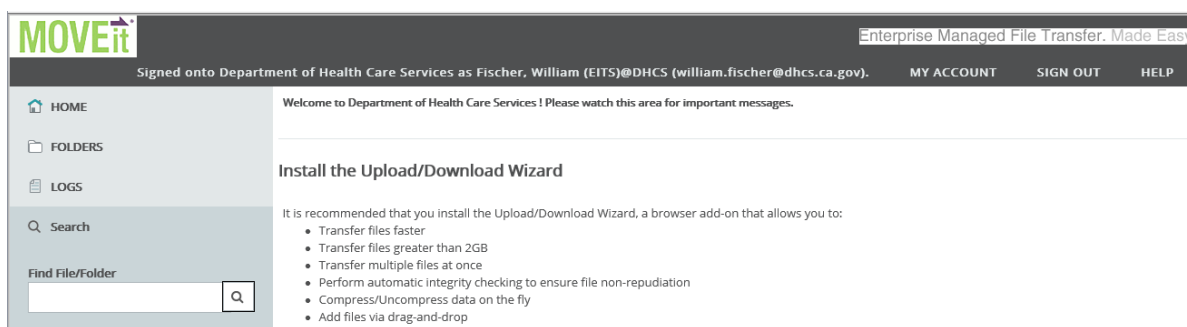


Figure I2: MoveIT File Transfer Home Page

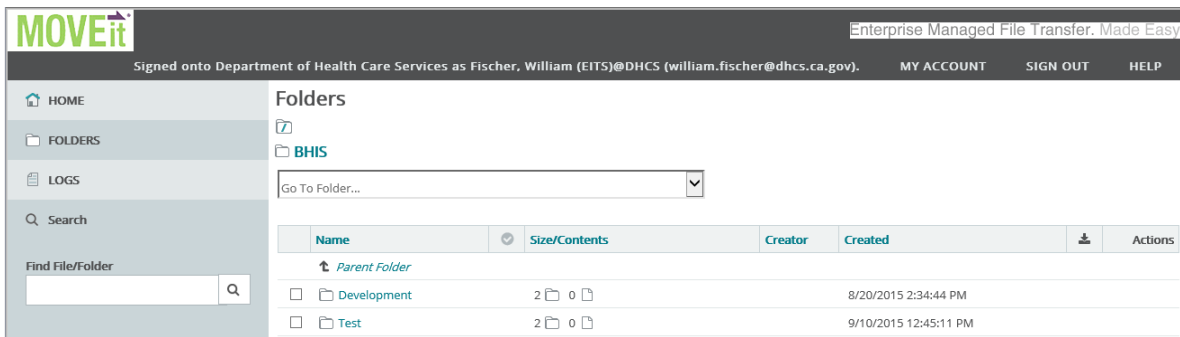


Figure I3: MoveIT File Transfer Production and Test Folders

Counties and Direct Providers who have access to multiple systems will be able to see each folder associated with those systems alongside of the **SDMC** folder. (See figures I4)

Name	Size/Contents	Creator	Created	Actions
Parent Folder				
CFRS	2 folders, 0 files		6/4/2019 3:36:47 PM	
SDMC	3 folders, 0 files		5/23/2019 3:43:57 PM	

Figure I4: MoveIT File Transfer System Folders

SDMC Users who submit data for both **Mental Health (DMH)** and the **Alcohol & Drug Program (ADP)** will be able to access both. Otherwise, they will only see the folder for the program they're under, and a folder for accessing any **System Documentation** which is replicated in all system folders. (See figures I5)

Name	Size/Contents	Creator	Created	Actions
Parent Folder				
ADP	1 folder, 0 files		5/23/2019 3:43:57 PM	
DMH	1 folder, 0 files		5/23/2019 3:45:03 PM	
SystemDocumentation			5/23/2019 3:45:03 PM	

Figure I5: MoveIT File Transfer SDMC Folders

Within either **Program** folder, a **SDMC User** will only see the folder for the **County** or **Direct Provider** that they represent. (See figures I6)

Name	Size/Contents	Creator	Created	Actions
Parent Folder				
SAN FRANCISCO-38	3 folders, 0 files		5/23/2019 3:45:33 PM	

Figure I6: MoveIT File Transfer County & Direct Provider Folders

The **County/Direct Provider** folder will contain the **Upload** folder for submitting new medical claims data files, the **Download** folder for accessing their **Snip Reports (SR)**, **999s**, **835s**, and **Transaction Acknowledgments (TA1)**, and the **Data Exchange** folder for accessing any special reports or data requests made for the county. (See figures I7)

Name	Size/Contents	Creator	Created		Actions
↑ Parent Folder					
<input type="checkbox"/> DataExchange			5/23/2019 3:45:33 PM		
<input type="checkbox"/> Download			5/23/2019 3:45:33 PM		
<input type="checkbox"/> Upload			5/23/2019 3:45:33 PM		

Figure I7: MoveIT File Transfer Upload, Download, and Data Exchange Folders

CAUTION: All county files placed in the **Download** folder will only be held there for up to **45** days before they are **purged**!

NOTE: Many of the MoveIT folders can be accessed immediately using the **Go To Folder** dropdown

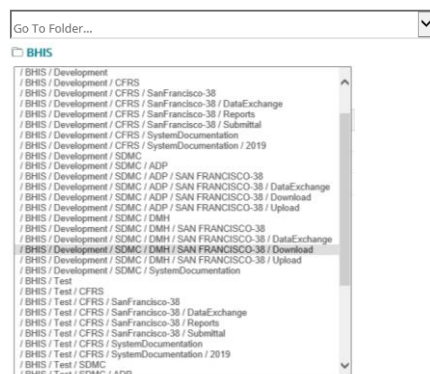


Figure I8: MoveIT File Transfer Go To Folder Dropdown List

Contacting SDMC Support

DHCS IT Service Desk Support

For any technical questions involving the creation of an **O365 AAD** account, submitting a new **Email Domain** to be whitelisted by **DHCS**, issues with accessing the **SDMC Application**, or uploading or downloading files to or from the **MoveIT File Transfer Service**, or just general questions and assistance, then please feel free to contact **DHCS** by email at ITServiceDesk@dhcs.ca.gov, or by phone at **(916) 440-7000**.

MEDCCC Support

For any assistance with certifying new **Approvers** for the **SDMC** system, enrolling for **Electronic Funds Transfer**, or determining why a submitted claim was rejected, then please contact **DHCS** by email at MEDCCC@dhcs.ca.gov.