COMMONWEALTH of VIRGINIA

Department of Medical Assistance Services

Web Portal
Provider Registration
Users Guide

Version 7.0
Revision Date: 08/11/2015

HIPAA Privacy Rules

The Health Insurance Portability and Accountability Act of 1996 (HIPAA – Public Law 104-191) and the HIPAA Privacy Final Rule[1] provides protection for personal health information. The regulations became effective April 14, 2003. Xerox developed HIPAA Privacy Policies and Procedures to ensure operations are in compliance with the legislative mandate.

Protected health information (PHI) includes any health information whether verbal, written, or electronic, that is created, received, or maintained by Xerox. It is health care data, plus identifying information that allows someone using the data to tie the medical information to a particular person. PHI relates to the past, present, and future physical or mental health of any individual or recipient; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. Claims data, prior authorization information, and attachments such as medical records and consent forms are all PHI.

The Privacy Rule permits a covered entity to use and disclose PHI, within certain limits and providing certain protections, for treatment, payment, and health care operations activities. It also permits covered entities to disclose PHI without authorization for certain public health and workers' compensation purposes, and other specifically identified activities.
[1]

---

[1] 45 CFR Parts 160 and 164, Standards for Privacy of Individually Identifiable Health Information; Final Rule

Revision History

Document Version	Date	Name	Comments
1.0	05/15/2010	Xerox Transition Web Portal Team	Initial Document Creation
2.0	06/06/2010	Xerox Transition Web Portal Team	Revisions made based on comments received from DMAS
2.1	6/19/2010	Xerox Transition Web Portal Team	Additional revisions made based on comments received from DMAS
3.0	8/30/2011	Xerox Web Portal Team	Corrections and post go-live updates
3.1	4/16/2012	Xerox Web Portal Team	Rebranding – ACS to Xerox
4.0	12/19/2014	Xerox Web Portal Team	Updates based on Release 71
5.0	02/02/2015	Xerox Web Portal Team	Updates based on DMAS comments for Release 71
6.0	02/20/015	Xerox Web Portal Team	Updates based on Release 71 modifications
7.0	08/11/2015	Xerox Web Portal Team	Updates based on MSR 2015-219-001-W

Table of Contents

0.0 Introduction

The Commonwealth of Virginia's Medicaid Web Portal is a web based system that gives providers and their user organizations access to secured provider services.

The Portal extends the business capabilities of Virginia providers by offering user-friendly tools and resources. You will have access to the secured interactive features of the portal including:

- Claims Status Inquiry

- Claims Direct Data Entry

- Member Eligibility, Co-Pay Amounts and Member Service Limits

- Service Authorization Log and Pharmacy Web PA Request

- Provider Payment History

- EHR Incentive Program

- Remittance Advice (RA) Messages

- Provider Maintenance

- Provider Enrollment

- Level of Care Review

- Pre-Admission Screening

In order to take advantage of the Portal and its functions, users must be part of the security structure.

For the sake of this document, a 'user' is defined as any person that will access and use the Web Portal.

If at any time during the registration process you have questions or issues, please contact the Virginia Medicaid Helpdesk toll free at 866-352-0496.

0.1   Security Structure

The security structure of the Web Portal is provider centric. Security access for the Web Portal is based upon a provider organization. A 'provider organization' is defined as either an individual billing or servicing provider or group provider (and the user community in support of them).

The provider organization can be associated with either a NPI (National Provider Identifier) or an API (Atypical Provider Identifier – assigned by the Commonwealth of Virginia for providers that are not eligible for a NPI, such as a transportation provider).

A unique User ID will need to be established for each provider organization a user supports. Any users added to the organization will have the ability to access services based on the role they are assigned.

0.2   User Roles

There is a three-tiered security structure associated with each provider organization. Additional roles may be provided as new services are added.

Primary Account Holder – A Primary Account Holder is the person who will perform the initial web registration. He/she will establish the security needed for the services accessed.

Each provider organization can have only one Primary Account Holder.   Any change to the Primary Account Holder (PAH) must be made in writing by completing and faxing the Primary Account Holder Change Form into the Virginia Medicaid Web Support Helpdesk. The Primary Account Holder Change form and instructions for completing can be found under Web Registration Reference Material.

The Primary Account Holder can
- Establish Organization Administrators and/or Authorized Users for their organization
- Change roles for any user
- Reset passwords for any user
- Activate and/or deactivate any user
- Unlock any User ID
- Access to all secured provider functionality including:
    - Access to Claims Direct Data Entry
    - Access to Provider Profile Maintenance

Organization Administrator – An Organization Administrator is established by the Primary Account Holder.

An Organization Administrator is not required for a provider organization - some organizations may only have a Primary Account Holder and associated Authorized Users. A provider organization can have one-to-many Organization Administrators, if so desired. Organization Administrators tier up to the Primary Account Holder.

The Organization Administrator has the following capabilities associated with only Authorized Users:
- Can establish Authorized Users for their organization
- Can change roles for any Authorized User
- Can reset passwords for any Authorized User
- Can activate and/or deactivate any Authorized User
- Can unlock any Authorized User ID
- Access to all secured provider functionality including:
    - Access to Claims Direct Data Entry
    - Access to Provider Profile Maintenance

Authorized User - The Authorized User is responsible for performing provider support functions.

Authorized Users are not required for a provider organization, but an organization can have one-to-many Authorized Users, if so desired. Authorized Users tier up to the Organization Administrators.

The Authorized User has the following capabilities:
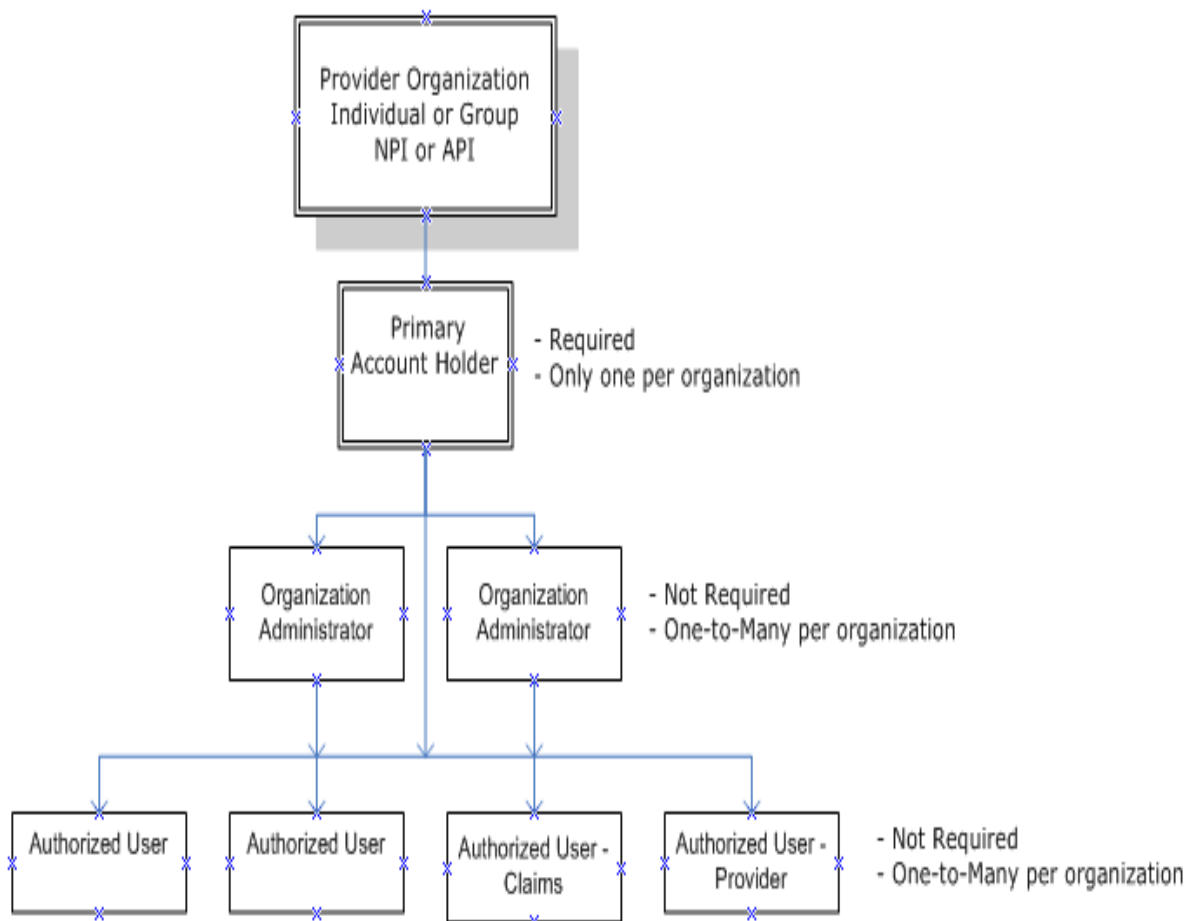- Has access to all ARS secured provider functionality

Authorized User – Claims – The Authorized User – Claims role is established by either the Primary Account Holder or Organization administrator for performing claims submission on behalf of the provider organization.

The Authorized User - Claims role is not required for a provider organization, but an organization can have one-to-many Authorized User - Claims, if so desired. Authorized User - Claims tier up to the Organization Administrators.

The Authorized User – Claims has the following capabilities:
- Can submit claims through the Claims Direct Data Entry (DDE)
- Has access to all ARS secured provider functionality

Authorized User – Provider – The Authorized User – Provider role is established by either the Primary Account Holder or Organization administrator for performing demographic, disclosure and revalidation updates on behalf of the provider organization, using the Provider Maintenance functionality.

The Authorized User - Provider role is not required for a provider organization, but an organization can have one-to-many Authorized User – Provider roles, if so desired. The Authorized User - Provider tier up to the Organization Administrators.

The Authorized User – Provider has the following capabilities:
- Can make updates to the provider's demographic information, including:
  - Updates to correspondence information
  - Updates to remittance information
  - Updates to pay-to information
  - Note: updates to service information for most provider types will still be submitted via the enrollment process
  - Updates to disclosure information
  - Revalidation verification (when due)
- Has access to all secured provider functionality

Within the provider organization's security structure, the users within each tier are accessible within the system to all users in the tiers above. All Authorized Users can be accessed and user maintenance performed for them by all Organization Administrators and the Primary Account Holder.

The following reflects the security structure for each provider organization.

Provider Organization's
Security Structure

Provider Organization
Individual or Group
NPI or API

Primary
Account Holder
- Required
- Only one per organization

Organization
Administrator

Organization
Administrator
- Not Required
- One-to-Many per organization

Authorized User

Authorized User

Authorized User -
Claims

Authorized User -
Provider
- Not Required
- One-to-Many per organization

0.3   Overall Registration Process

The Web Registration process for new provider organizations must be completed by the Primary Account Holder.

The registration process involves the following five steps:

1. Establish a User ID, Password and security profile
2. Request secured access for your organization
3. Successfully complete a one-time verification process of 3 questions
4. Upon receipt of confirmation email, click link within email
5. Sign in to the secured portal

Step 1 - Establish a User ID, Password and Security Profile

As the Primary Account Holder you must first create a User ID and password and answer three unique security questions which will enable you to access the system if you forget your User ID or password

For more details, please see 2.3 *Creating a User Profile* or *2.6 Creating a Security Profile*.

Step 2 – Request Secured Access for your Organization

Note: If you are associated with a provider not currently enrolled in the Virginia Medicaid program, you will need to wait for Provider Enrollment Services to approve the application before requesting secured access.

The Primary Account Holder will request secured access by clicking the 'Request Security Access' in the Quick Links or the link 'Request Secured Access' within the Welcome page. Your security profile will be displayed along with three validation questions.

Step 3 - Successfully complete a one-time verification process of 3 questions

You will be required to select three unique questions from the provider related questions. Complete answers as they relate to the NPI associated to the organization. After clicking 'Submit' the answers will be validated against the information on the VA MMIS. If validation is unsuccessful, you will need to contact the provider for accurate answers and re-request secured access. If validation is successful, you will receive a confirmation message and an email will be generated and sent to your email address.

Step 4 - Upon receipt of confirmation email, click link within email

Upon receipt of the confirmation email, click on the link within it. This link will navigate you to the web portal sign in screen.

For more complete instructions, please refer to *3.0 Requesting Secured Access*.

Step 5 - Sign in to the secured portal

Signing in to the web portal will activate the secured access for you and the rest of the provider's organization.

Note: The purpose of the email is to ensure you log off and log on again after registration is complete. This will initiate the secured access. You can do this without waiting for the email if you wish.

You should now see all secured functionality (i.e. Claims Status, Member Eligibility, etc.). If not, please contact the Web Portal Support help desk at 866-352-0496.

If you haven't done so already, you can begin/continue creating (or modifying) your user organization. Click 'Add New Users' or 'View/Edit Users' from the Quick Links on the left side of the portal page. For more complete instructions, please refer to *5.0 Establishing a User Organization*.

1.0 Web Portal Access

The Virginia Medicaid Web Portal can be accessed through the following link:
www.virginiamedicaid.dmas.virginia.gov

The Web Portal is available daily 24 x 7 with the exception of routine maintenance which will be posted in advance.

The Web Portal currently only supports Internet Explorer browser version 6 and higher. Versions 9 and above may need to utilize the following:

Note for Internet Explorer 9 (or greater) users:

In order to use IE9 for the Web Portal the following settings are suggested:

- Security settings set to Medium-High

   a. Open an IE9 browser session
   b. Click Tools->Internet Options.
   c. Click the Security Tab
   d. Verify/change to Medium-High
- Verify Java is installed
   a. Go to www.java.com
   b. Press the option that says "Do I have Java?"
   c. Once the page refreshes, if Java is installed, the Java version will be displayed.
   d. If Java is not installed, press the free java download button.

- Add Virginia.gov to Compatibility View Settings
   a. Open an IE9 browser session
   b. Click Tools->Compatibility View settings.
   c. Type 'virginia.gov' and click 'Add'.
   d. Click 'Close'
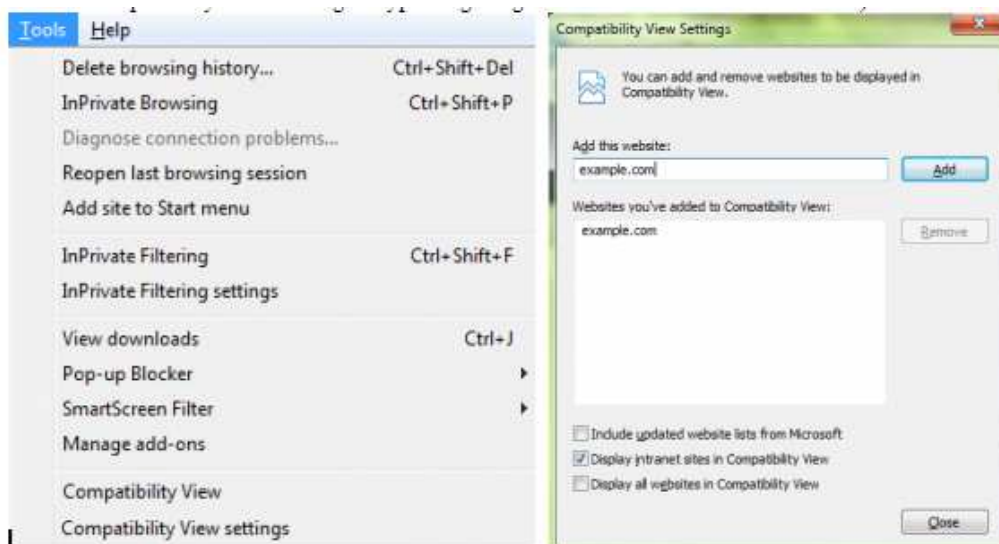
If at any time during the registration process you have questions or issues, please contact the Virginia Medicaid Helpdesk toll free at 866-352-0496.

The following sections will outline the basic functionality of the portal.

1.1 Medicaid Web Portal – Home Page

The Commonwealth of Virginia Medicaid Web Portal's home page contains various portlets (sections within a portal page) and navigational tabs.

The Web Portal's Home Page is reflected below:

1.1.1 Navigation Tabs

Provider Services – This tab provides access to the following:

- Provider Enrollment – access to provider enrollment applications for downloading
- Provider Manuals – access to provider manuals, service center user manuals, dental manuals and forms
- Medicaid Memos to Providers – Medicaid Memorandums from DMAS to the provider community
- DMAS Provider Services – link to Provider Services on the Department of Medical Assistance Services web site
- DMAS Pharmacy Services – link to Pharmacy Services on the Department of Medical Assistance Services web site

Provider Resources – This tab provides access to the following:

- Provider Manuals – access to provider manuals, service center user manuals, dental manuals and forms
- Provider Links – links to Center of Medicare and Medicaid Services, DMAS and Virginia.gov websites
- Provider Training – access to the provider training library

- Web Registration – access to Registration FAQ, a Registration Quick Reference Guide, this Registration User's Guide and access to the Registration tutorial
- Automated Response System (ARS) – access to the ARS Users Guide, ARS FAQ and ARS tutorials
- Claims DDE – access to the Claims DDE Users Guide, Claims DDE FAQ and Claims DDE tutorial
- Provider Maintenance – access to the Provider Maintenance Users Guide, Provider Maintenance FAQ and Provider Maintenance tutorial
- Search for Provider – access to the VA MMIS Search for Providers to search for providers by provider type, location, etc.
- Level of Care Review Instrument (LOCERI) – access to the LOCERI User Guide, LOCERI FAQ and the LOCERI tutorial
- Provider Enrollment Resources – access to the Provider Enrollment Users Guide, Provider Enrollment FAQ and Provider Enrollment tutorial
- Provider Screening and Fee Rpt – access to the report for State Medicaid Agencies that want to verify screenings and fees.
- ICD-10 – access to the Information and Frequently Asked Questions and the Testing Procedures
- Pre-Admission Screening – access to the Pre-Admission Screening User Guides, Pre-Admission Screening FAQ and Pre-Admission Screening tutorial

EDI Support – This tab provides access to the following:

- EDI Companion Guides – links to the EDI companion guides for support of EDI transactions
- EDI FAQ – Frequently Asked Questions on EDI transactions
- EDI Testing – Guidelines for EDI testing
- EDI Forms and Links – access to EDI forms and links
- EDI HIPAA Changes – access to the VAMMIS HIPAA Operating Rules Trading Partner Notification

Documentation – This tab provides access to the following:

- Provider Forms – access to various forms in support of provider services
- Paper Claim Forms – access to various claims forms for download

EHR Incentive Program – This tab provides access to information regarding the Virginia Medicaid EHR Incentive Program

FAQ – This tab provides access to the following:

- ARS FAQ
- Claims DDE FAQ
- Provider Maintenance FAQ
- Provider Enrollment FAQ

- EDI FAQ
- Web Portal Registration FAQ
- VAMMIS File Transfer System FAQ
- Search for Providers FAQ
- Level of Care Review Instrument (LOCERI) FAQ
- ORP FAQ
- Pre-Admission Screening FAQ

Provider Enrollment - This tab furnishes providers access to the online provider enrollment applications, once logged in, or a link to the paper versio of the applications.

1.1.2 Home Page Portlets – Web Announcements

Web Announcements – this portlet contains any information that is applicable to all portal users such as maintenance down time, new policies, etc.

1.1.3 Home Page Portlets – Quick Links

Quick Links – this portlet list links to documents or websites that are applicable to the audience viewing this portal page. Quick Links will be located on various portal pages. For consistency and availability to common information, the first five (5) links will always be the same as the navigation tabs:

- Provider Services
- Provider Resources
- EDI Support
- Documentation
- FAQ

In addition there are links that are applicable to that portal page.

For the Home Page, the additional quick links are the following:

- **EHR Incentive Program** – access to information regarding the Virginia Medicaid EHR Incentive Program
- **Search for Providers** – access to the VA MMIS Search for Providers to search for providers by provider type, location, etc.
- **Provider Forms Search** – access to the provider forms with the capability to limit searches by category, form type, etc.
- **Web Registration Reference Material** - access to Registration FAQ, a Registration Quick Reference Guide, this Registration User's Guide and access to the Registration tutorial
- **DMAS Web Site** – link to the website for the Department for Medical Assistance Services

- **ICD-10** – access to the Information and Frequently Asked Questions and the Testing Procedures
- **DME and Pharmacy Audits** – access to information associated with DME and pharmacy audits and reports

1.1.4 Home Page Portlets – Login

This portlet is used for logging in to the pages needed for secured login. The login choice is based upon the user's role. For registration and access to secured provider functionality, select the 'Provider' role.

1.2 Medicaid Web Portal – Provider Login Page

After selecting the 'Provider' role in the Web Portal Home Page, the provider and the supporting user community are directed to the Provider Login Page.

The Provider Login Page is reflected below:

There are three portlets on this page different from the Web Portal Home Page.
- Welcome portlet
- First Time User Registration portlet
- Existing User Login portlet

1.2.1 Welcome Portlet

The Welcome portlet is reflected below:
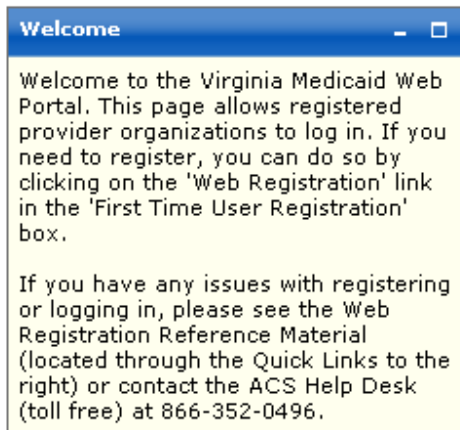
This portlet contains general instructions as well as mechanisms to handling issues or questions:

- Web Registration Reference Material – from the quick links
- Virginia Medicaid Help Desk – toll free number

1.2.2 First Time User Registration Portlet

The First Time User Registration portlet is reflected below:

First Time User Registration — ▭

By registering you will be designated as the Primary Account Holder for your organization. As the designated Primary Account Holder, you can add, delete or modify user access.

If you are currently a user supporting an organization associated with a Medicaid provider enrolled with the Department of Medical Assistance Services, then as a new Primary Account Holder registrant, you must complete the following steps:
1. Establish a User ID, Password and security profile
2. Request secured access for your organization
3. Successfully complete a one-time verification process of 3 questions
4. Upon receipt of confirmation email, click link within email
5. Sign in to the secured portal

If you are a user supporting an organization associated with a provider who is registering in order to submit a Medicaid enrollment application, then as a new Primary Account Holder registrant, you need only complete the following step:
1. Establish a User ID, Password and security profile

After the enrollment application is approved, you must then complete the remaining registration steps noted below:
2. Request secured access for your organization
3. Successfully complete a one-time verification process of 3 questions
4. Upon receipt of confirmation email, click link within email
5. Sign in to the secured portal

If you are not the Primary Account Holder for your organization then you should not register. If your organization already has a Primary Account Holder, please see them for your User ID and Password to log in.

◉ Web Registration

This portlet outlines the steps needed for completing the registration process. Only the user designated as the Primary Account Holder should complete the registration process.
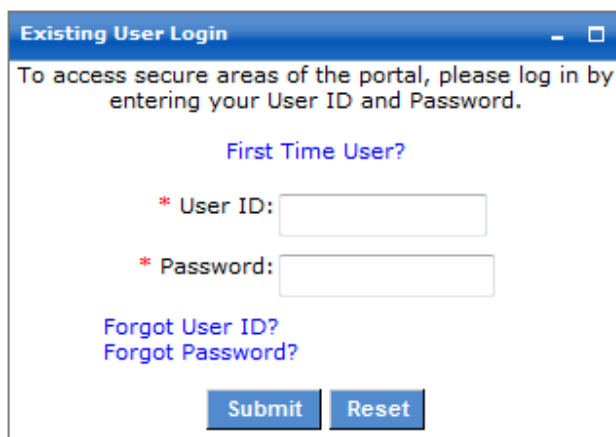
Users that are not designated as the Primary Account Holder should contact their Primary Account Holder or Organization Administrator for their User ID and temporary password.

As the Primary Account Holder, not previously registered, you'd select 'Web Registration' link on this portlet.

1.2.3 Existing User Login Portlet

Once you have established your User and Security Profiles, you will have access to the public portal functionality for such things as access to online provider enrollment or requesting secured access to other portal functionality.

The Existing User Login portlet is reflected below:

First Time User? – For users that have not registered for the portal, this link will take you to the start of the registration process.

This portlet is used for applying a registered user's User ID and password. Both are required fields (indicated with a red asterisk *) for the login process.

User ID – this is the User ID created during the registration process when establishing your User Profile (see Registration Users Guide).

Password – this is the Password created during the registration process when establishing your User Profile.

Enter your User ID and Password and click 'Submit'

The Forgot User ID and Forgot Password are addressed in further detail below

1.3 Log Out

The log out functionality is available on any secured web portal page. The
Log Out link is reflected below:

If you are not logged in and are still on public pages, this link is not available
as it's not applicable until you've accessed secured portal pages.

2.0 Registration Process

2.1 Who Can Register?

Only the user designated as the Primary Account Holder should complete the registration process.

Users that are not designated as the Primary Account Holder should not register and should contact their Primary Account Holder or Organization Administrator for their User ID and temporary password.

2.2 Why Would I Need to Register?

In order to gain access to the secured provider functions such as member eligibility and service limits, claims status inquiry, service authorization inquiry and payment history, claims direct data entry and/or provider maintenance (for updating provider demographics or completing revalidation), you will need to be a registered portal user. By registering, and Requesting Secured Access, the system has the mechanism to authenticate you as the Primary Account Holder.

Once authenticated, you will be able to establish your provider organization. Doing so will give all the users within your organization the access to secured functionality, based on their specific role.

2.3 Creating a User Profile

Once you've clicked on 'Web Registration' from the First Time User Registration portlet, or 'First Time User' from the login portlet (see sections 1.2.2 First Time User Registration Portlet or 1.2.3 Existing User Login Portlet) you will be directed to the User Profile.

The User Profile portal page is reflected below:

The User Profile is part of the registration process and contains the following information. Any information that is required (noted with a red asterisk *) will need to be supplied by you at the initial login. Any optional fields that are known are recommended to be completed at this time as well.

- Provider ID (NPI/API)
- User ID *
- NPI's FEIN
- Password *
- First Name *
- Last Name *
- Middle Initial
- Phone Number *
- Extension
- Preferred email *

Provider ID (NPI/API) (optional) – Though this field is not a required field at this point, in order to complete the authentication process your User ID will need to be associated to an individual or group NPI (or API).

If the NPI (or API) is known at this time, it should be entered at this time.

In the case of an atypical provider, an API number might not yet be assigned. The authentication process can not be completed until the NPI or API is entered, but the User and Security Profiles can be established in the interim.

Create User ID * (required) **–** You will need to establish a unique User ID that will be associated with this individual or group provider.

The User ID must be a minimum of 6 characters and a maximum of 16 characters. It can include hyphens, underscores or periods. The User ID can not start with special characters nor can it contain spaces.

FEIN (optional) - Enter the FEIN associated with the individual or group provider

Create Password * (required) – Establish a password to be used in conjunction with your User ID to authenticate you at the time of login.

The portal password must be a minimum of 8 characters and must include three (3) of the following four (4) requirements:

- Capital/Upper case letter
- Lower case letter
- Number
- Special character (!, $, #, %)

Re-type Password * (required) – Re-enter the password from the 'Create Password' box as a secondary check

First Name * (required) – Enter your first name

Last Name * (required) – Enter your last name

Middle Initial (optional) – Enter your middle initial

Phone Number * (required) – Enter your contact phone number

Ext (Extension) (optional) – If the phone number entered is a work number with a corresponding extension, enter the extension here

Preferred E-mail * (required) – Enter the email address where you wish to receive messages. This will be used only for sending temporary passwords in the case of a forgotten password or sending the User ID associated to this provider in the case of a forgotten ID

After completing all required and known/applicable optional fields, click on 'Continue'.

You will be taken to the Security Profile to continue the registration process.

2.4 Creating a Security Profile

The Security Profile is used to gather three (3) different security questions. These questions will be used for user self-help with forgotten passwords and User IDs.

The User Profile portlet is reflected below:

You will need to complete all three security questions. Each question must be unique.

The question choices are as follows:

- What is your Pet's Name?
- Where did you meet your spouse?
- Who was your childhood hero?
- What is your favorite pastime?
- What is your favorite sports team?
- What is your father's middle name?
- What is your high school mascot?
- What make was your first car or bike?

After completing the three security questions, click 'Submit' to complete your Security Profile. This completes the registration process.

You will be taken to the Primary Account Holder's Welcome Page (below). This page will let you start the second step in the authentication process, Request Secured Access, or log out to return later.

Jan 6, 2015

| Home | Contact Us | Log out

Virginia Medicaid

| Home | EHR Incentive Program | Provider Enrollment | Level of Care Review ▶ | Pre-Admission Screening ▶ |
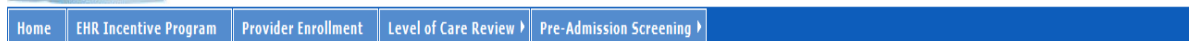
Quick Links

- Provider Services
- Provider Resources
- EDI Support
- Documentation
- FAQ
- Newborn E-213
- Hospital Presumptive Eligibility
- Search for Providers
- Provider Forms Search
- DMAS Web Site
- Change Password
- Request Secured Access
- Add Users
- View/Edit Users

News

Welcome to the Virginia Medicaid Web Portal.

If you have any issues continuing with the registration process, please see the Web Registration Reference Material (located at the Provider Resources Quick Links above) or contact the Virginia Medicaid Web Support Help Desk (toll free) at 866-352-0496.

Welcome to the Virginia DMAS Medicaid Web Portal

Thank you for registering for access to the Virginia Medicaid Web Portal. You've successfully completed the first step in the registration process.

If registering in order to enroll as Medicaid provider, please click here to be routed to the online application functionality: Provider Enrollment Application

As the Primary Account Holder for your organization, you will need to initiate and complete the authentication process for access to secured functionality. For more complete instructions, please refer to the Web Registration Quick Reference

After the enrollment application is approved, you must then complete the remaining registration steps below. While waiting for completion of the enrollment process, you may begin to establish your organization. To begin creating (or modifying) a user organization, click 'Add New Users' or 'View/Edit Users' from the Quick Links on the left. For more complete instructions, please refer to the Quick Reference for Establishing a Provider Organization. Once secured access is gained, all users associated with the provider organization will have the secured access associated to their security role.

If you are a new user associated with a provider not currently enrolled in the Virginia Medicaid Program, you will need to wait for Provider Enrollment Services to approve your application before you can request secured access.

Step 2 - Request secured access for your organization - click here to Request Secured Access or on the Request secured access link in the Quick Links on the left. Your security profile will be displayed along with three validation questions.

Step 3 - Successfully complete a one-time verification process of 3 questions - select three unique questions from the provider related questions. Complete answers as they relate to the NPI associated to the organization. After clicking 'Submit' the answers will be validated against the information on the Medicaid provider files. If validation is unsuccessful, you will need to contact the provider for accurate answers and re-request secured access. If validation is successful, you will receive a confirmation message and an email will be generated and sent to your email address.

Step 4 - Upon receipt of confirmation email, click link within email - upon receipt of the confirmation email, click on the link within it. This link will navigate you to the web portal sign in screen.

Step 5 - Sign in to the secured portal - signing in to the web portal will activate the secured access for you and the rest of the provider's organization. You should now see all secured functionality (i.e. Claims Status, Member Eligibility, etc.). If not, please contact the Web Portal Support help desk at 866-352-0496.

If you haven't done so already, you can begin/continue creating (or modifying) your user organization. Click 'Add New Users' or 'View/Edit Users' from the Quick Links on the left. For more complete instructions, please refer to the Quick Reference for Establishing a Provider Organization.

2.5 Forgot User ID

Once you've completed your User and Security Profiles, you are able to leverage the user self help capabilities of the portal. Authorized Users who forget their User ID can get with their Primary Account Holder or any Organization Administrator associated with this provider organization. They have the capability to look up the User IDs. An Organization Administrator can check with the Primary Account Holder.

All roles have the ability to also request their User ID be emailed to them.

On the Provider Login Page, in the Existing Users Login portlet there is an option for Forgot User ID?

Select 'Forgot User ID?'

Enter your Email Address: - this must be the preferred email that was entered in your User Profile at the time of initial entry (or the last update to your User Profile).

Provider ID (NPI/API): - enter the NPI or API associated with your User ID

Click 'Continue' and you will be routed to the portlet below.

This portlet will display the three questions you chose when establishing your Security Profile.

You must complete all three of these questions, giving the same answers (case sensitive) as you established in your Security Profile.

Upon completing the answers, click 'Continue' to invoke the validation of answers to your Security Profile.

After successful validation you will receive the following portlet:

Your User ID will be emailed to the email address entered in your User Profile.

The following is a sample email with the User ID removed:

Your Forgot User ID request has been processed.

Your User ID is :

Please use this to log in to the Virginia Medicaid Web Portal at
https://www.virginiamedicaid.dmas.virginia.gov .Please contact the ACS Web Support Call Center, toll free, at 1-866-352-0496 if you have any questions or problems regarding your web portal registration.

Note: This is an auto-generated email, please do not reply.

2.6 Forgot Password

Once you've completed your User and Security Profiles, you are able to leverage the user self help capabilities of the portal. Authorized Users who forget their password can get with their Primary Account Holder or any Organization Administrator associated with this provider organization. They have the capability to generate a temporary password. An Organization Administrator can check with the Primary Account Holder.

All roles have the ability to also request their password be emailed to them.

On the Provider Login Page, in the Existing Users Login portlet there is an option for Forgot Password?

Select 'Forgot Password?'

Enter your User ID: - enter your User ID created in your User Profile

Click 'Continue' and you will be routed to the following portlet:

This portlet will display the three questions you chose when establishing your Security Profile.

You must complete all three of these questions, giving the same answers (case sensitive) as you established in your Security Profile.

Upon completing the answers, click 'Continue' to invoke the validation of answers to your Security Profile.

After successful validation you will receive the following portlet:

A temporary/one-time use password will be emailed to the email address entered in your User Profile.

The following is a sample email:

This temporary password will be used for login. You will immediately be taken to your User Profile and will be required to enter another password.

3.0 Requesting Secured Access

3.1 Why Do I Need to Request Secured Access?

As the Primary Account Holder for your organization, you will need to initiate and complete the authentication process.

Requesting Secured Access is a one-time process to be completed only by the Primary Account Holder.

3.2 Accessing the Security Profile

To request secured access, you will need to access the Primary Account Holder Welcome Page. After completion of the Security Profile, you will be immediately taken to this page (see section 2.4 Creating a Security Profile).

If you've logged out after completing the Security Profile the following steps will direct you back to the Primary Account Holder Welcome Page.
- On the Medicaid Web Portal Home Page – select 'Provider' from the Login portlet
- On the Provider Login Page – enter your User ID and password in the Existing User Login
- You will be directed to the Primary Account Holder Welcome Page

From this page there are two options for requesting secured access. On the Quick Links to the left is a link to 'Request Secured Access'. In the Welcome verbiage, Step 2 also contains the link to 'Request Secured Access.'

Clicking on the 'Request Secured Access' link will direct you to your Security Profile.

3.3   Requesting Secured Access

If the NPI/API was not previously entered, it will be required before further processing can be completed.

The following screen will display:

Enter the associated NPI/API and click 'Submit'.

After successfully including the NPI/API or if the NPI/API was entered initially, the following screen will display. This is a one-time authentication process conducted by the Primary Account Holder.

The PAH will be required to complete three questions. The first question will require either the provider's SSN or FEIN. Drop down options will be based on what information is captured in the MMIS.

Validation Question 1 could contain the following drop down values:

- Provider's SSN (last 4 digits)
- Provider's FEIN (last 4 digits)

Note: The NPI in this example has no SSN currently housed in the MMIS so only the FEIN selection will appear.

Validation Questions 2 and 3 will contain a list of provider information available on the MMIS. The user can select any question available in the drop down. Question 2 and 3 must be different though.

Possible Question options (unless the information is not on the MMIS for the provider secured access is being requested for):

- License End Year (YYYY)
- Provider's birth year (YYYY)
- Zip Code of Provider's Correspondence Address
- Bank Routing Number (last 4 digits)
- Bank Account (last 4 digits)
- EDI Submitter ID

Screen sample below contains questions with information for the provider entered in this example.

If validation is unsuccessful, you will receive the following error message:

The secured access for your provider organization has not been validated. Question(s) <<1, 2, 3>> has/have been answered incorrectly. Please correct your answers or contact the provider for information to correctly complete. If you have any additional questions, please contact the Web Portal support help desk at 866-352-0496.

Upon successful authentication of the questions entered, the following screen will display:

3.4   Secured Access Confirmation Email

A Secured Access Confirmation will be sent via email to the Primary Account Holder's email address.

Upon receipt, the PAH will need to click the link within the email. Signing in to the web portal will activate the secured access for you and the rest of the provider's organization.

Note: The purpose of the email is to ensure you log off and log on again after registration is complete. This will initiate the secured access. You can do this without waiting for the email if you wish.

You should now see all secured functionality (i.e. Claims Status, Member Eligibility, etc.). If not, please contact the Web Portal Support help desk at 866-352-0496.

If you haven't done so already, you can begin/continue creating (or modifying) your user organization. Click 'Add New Users' or 'View/Edit Users' from the Quick Links on the left side of the portal page. For more complete instructions, please refer to *5.0 Establishing a User Organization*.

A sample confirmation email is below:

From:	providerenrollmentreceipt@dmas.virginia.gov		Sent: Mon 12/15/2014 1:04 PM
To:			
Cc:			
Subject:	Secured Access Confirmation Email		

12/15/2014

To:

Your request for secured portal access on behalf of NPI _____ has been successfully validated.

In order to complete the access process, please click the link below. This will open up a new browser window, displaying the Virginia Medicaid provider portal sign on page.

Logging in to the portal with your User ID and password will complete the secured access process. All users currently part of your provider organization, or any that will be added, will automatically have secured access, based on their designated role, once this process is complete.

Virginia Medicaid Provider Portal Log In:
https://www.virginiamedicaid.dmas.virginia.gov/wps/portal/ProviderLogin

Note: Please do not respond to this automated email. If you encounter any issues completing this process, please refer to the Registration User Guide on the portal (under the Provider Resources tab >> Registration Reference Material) or contact the Web Portal Support help desk at 866-352-0496 for further assistance.

4.0 Accessing Secured Functionality

Once the authentication process is complete, the secured access will apply to automatically to any user within the NPI organization. Anyone already added or to be added.

To access secured functionality, users will need to log in to the portal.

- On the Medicaid Web Portal Home Page – select 'Provider' from the Login portlet
- On the Provider Login Page – enter your User ID and password in the Existing User Login
- You will be directed to Provider Secured Home Page

4.1 Provider Secured Functions

Once authenticated, you and any user you've established within your provider organization will have access to secured provider functions.

Tabs on the top of the page will navigate you to the following secured provider functions:

Claims – Claims Status Inquiry and Claims Direct Data Entry options
Member – Member Eligibility, Member CoPay and Member Service Limits
Service Authorization – Service Authorization Log
Payment History – Provider Payments
EHR Incentive Program – Information and Links associated with the EHR Incentive Program
Provider Maintenance – Provider Demographic Maintenance, Disclosure, Revalidations and Revalidation Status Tracking.
Provider Enrollment – Online applications for provider enrollment
RA Messages – RA messages available for providers receiving electronic remittances.
Level of Care Review - Level of Care Review Instruments
Pre-Admission Screening – Pre-Admission Screening forms, Status Tracking, File Upload and Assessment Search

For more details on these functions, please refer to the associated Reference Material (including Users Guides, FAQ and tutorials).

On the left within the Quick Links section are two maintenance links that any user can leverage.

Change Password – let's any user change their password
Change Security Profile – let's any user update their security questions

5.0 Establishing a User Organization

5.1 Accessing the Add Users Page

To begin establishing a user organization, you need to access the Provider Home Page.

- On the Medicaid Web Portal Home Page – select 'Provider' from the Login portlet
- On the Provider Login Page – enter your User ID and password in the Existing User Login
- You will be directed to the Provider Home Page

From the Quick Links on the left, click on the 'Add Users' link. The 'Add Users' link will only display for Primary Account Holders and Organization Administrators.

Clicking on the 'Add Users' link will direct you to the 'Add Organization Users' page.

Aug 30, 2011

Home | Contact Us | Log out

Virginia Medicaid

| Home | Claims ▸ | Member ▸ | Service Authorization ▸ | Payment History | Profile Maintenance |

Quick Links

- Provider Services
- Provider Resources
- EDI Support
- Documentation
- FAQ
- DMAS Web Site
- Change Password
- Change Security Profile
- Add Users
- View/Edit Users

Add Organization Users

* Required Field

Add User

Please enter the following information about the user you would like to add.

* User ID

Prefix   * Last Name   * First Name   MI   Suffix

* Phone / Ext   * Email

* Password   * Confirm Password

* What roles will this user have in the organization?

Available	Selected
OrganizationAdministrator AuthorizedStaff AuthorizedStaff - Claims AuthorizedStaff - Provider	

->>   ->   <-   <<-

Cancel   Reset   Add

5.2 Adding an Organization Administrator

You will need to complete a User Profile for the Organization Administrator you wish to add.

Any information that is required (noted with a red asterisk *) will need to be supplied. Any optional fields that are known are recommended to be completed at this time as well.

- User ID *
- Prefix
- Last Name *
- First Name *
- Middle Initial
- Suffix
- Phone Number *
- Extension
- Email *
- Password *
- Confirm Password *

User ID * (required) **–** You will need to establish a unique User ID for this Organization Administrator

The User ID must be a minimum of 6 characters and a maximum of 16 characters. It can include hyphens, underscores or periods. The User ID can not start with special characters nor can it contain spaces.

Prefix (optional) – Enter an applicable prefix from the drop down list

Last Name * (required) – Enter the Organization Administrator's last name

First Name * (required) – Enter the Organization Administrator's first name

Middle Initial (optional) – Enter the Organization Administrator's middle initial

Prefix (optional) – Enter the Organization Administrator's suffix if applicable

Phone Number * (required) – Enter the Organization Administrator's contact phone number

Ext (Extension) (optional) – If the phone number entered is a work number with a corresponding extension, enter the extension here

E-mail * (required) – Enter the email address where the Organization Administrator is to receive messages. This will be used only for sending temporary passwords in the case of a forgotten password or sending the OrgAdmn's User ID in the case of a forgotten ID

Password * (required) – Establish a temporary password to be used by the Organization Administrator to authenticate them at the time of initial login.

The portal password must be a minimum of 8 characters and must include three (3) of the following four (4) requirements:

- Capital/Upper case letter
- Lower case letter
- Number
- Special character (!, $, #, %)

Confirm Password * (required) – Re-enter the password from the 'Password' box as a secondary check

To select the role, you will utilize the roles tables. To establish the user as an Organization Administrator, select that role from the 'Available' roles. Use the single arrow -> (outlined below) to move the role from 'Available' to 'Selected'.

Note: If the wrong role is accidently selected, it can be moved back from the 'Selected' role to the 'Available' role column.

Once the desired role is in the 'Selected' column, click 'Add' to process the User ID.

When successfully added, you'll receive an appropriate message.

5.3 Adding Authorized Staff

To add another user, select 'Add Users' from the Quick Links to the left or if logging in to a new session, you will need to access the Provider Home Page.

- On the Medicaid Web Portal Home Page – select 'Provider' from the Login portlet
- On the Provider Login Page – enter your User ID and password in the Existing User Login
- You will be directed to the Provider Home Page
- Select 'Add Users' from the Quick Links to the left

You will need to complete a User Profile for any Authorized Staff you wish to add.

Any information that is required (noted with a red asterisk *) will need to be supplied. Any optional fields that are known are recommended to be completed at this time as well.

- User ID *
- Prefix
- Last Name *
- First Name *
- Middle Initial
- Suffix
- Phone Number *
- Extension
- Email *
- Password *
- Confirm Password *

User ID * (required) **–** You will need to establish a unique User ID for this Authorized User. This User ID will need to be relayed to the user by the Primary Account Holder or Organization Administrator.

The User ID must be a minimum of 6 characters and a maximum of 16 characters. It can include hyphens, underscores or periods. The User ID can not start with special characters nor can it contain spaces.

Prefix (optional) – Enter an applicable prefix from the drop down list

Last Name * (required) – Enter the Authorized User's last name

First Name * (required) – Enter the Authorized User's first name

Middle Initial (optional) – Enter the Authorized User's middle initial

Prefix (optional) – Enter the Authorized User's suffix if applicable

Phone Number * (required) – Enter the Authorized Users' contact phone number

Ext (Extension) (optional) – If the phone number entered is a work number with a corresponding extension, enter the extension here

E-mail * (required) – Enter the email address where the Authorized User is to receive messages. This will be used only for sending temporary passwords in the case of a forgotten password or sending the Authorized User's User ID in the case of a forgotten ID

Password * (required) – Establish a temporary password to be used by the Authorized Staff to authenticate them at the time of initial login. This initial

password will need to be relayed to the user by the Primary Account Holder or Organization Administrator, all subsequent password changes will be emailed to the user.

The portal password must be a minimum of 8 characters and must include three (3) of the following four (4) requirements:

- Capital/Upper case letter
- Lower case letter
- Number
- Special character (!, $, #, %)

Confirm Password * (required) – Re-enter the password from the 'Password' box as a secondary check

To select the role, you will utilize the roles tables. To establish the user as an Authorized User, select that role from the 'Available' roles. Use the single arrow -> (outlined below) to move the role from 'Available' to 'Selected'.

Note that there are three types of AuthorizedStaff roles. AuthorizedStaff (only) – will allow the user inquiry capability to the ARS functionality only. AuthorizedStaff – Claims will allow the user to submit claims via direct data entry as well as have inquiry capability to the ARS functionality. AuthorizedStaff – Provider will allow the user to update provider demographic information as well as have inquiry capability to the ARS functionality.

If a user needs to be able to submit claims as well as update the provider demographic information, you can select both the AuthorizedStaff – Claims

and the AuthorizedStaff – Provider roles. It's not necessary to also select the 'Authorized Staff' role with either of these already have that same inquiry functionality.

Note: If the wrong role is accidently selected, it can be moved back from the 'Selected' role to the 'Available' role column.

Once the desired role is in the 'Selected' column, click 'Add' to process the User ID.

When successfully added, you'll receive an appropriate message.

6.0 User Maintenance

Once you've established your organization, both the Primary Account Holder and any Organization Administrators have the ability to change a user's role, reset a forgotten password, activate or deactivate a user and unlock an ID that was locked for too many password tries.

To begin user maintenance, you need to access the Provider Home Page.

- On the Medicaid Web Portal Home Page – select 'Provider' from the Login portlet
- On the Provider Login Page – enter your User ID and password in the Existing User Login
- You will be directed to the Provider Home Page

6.1 Accessing the User Maintenance Page

From the Quick Links on the left, click on the 'View/Edit Users' link. The 'View/Edit Users' link will only be viewable to Primary Account Holders and Organization Administrators.

Clicking on the 'View/Edit Users' link will direct you to the 'Add Organization Users' page.
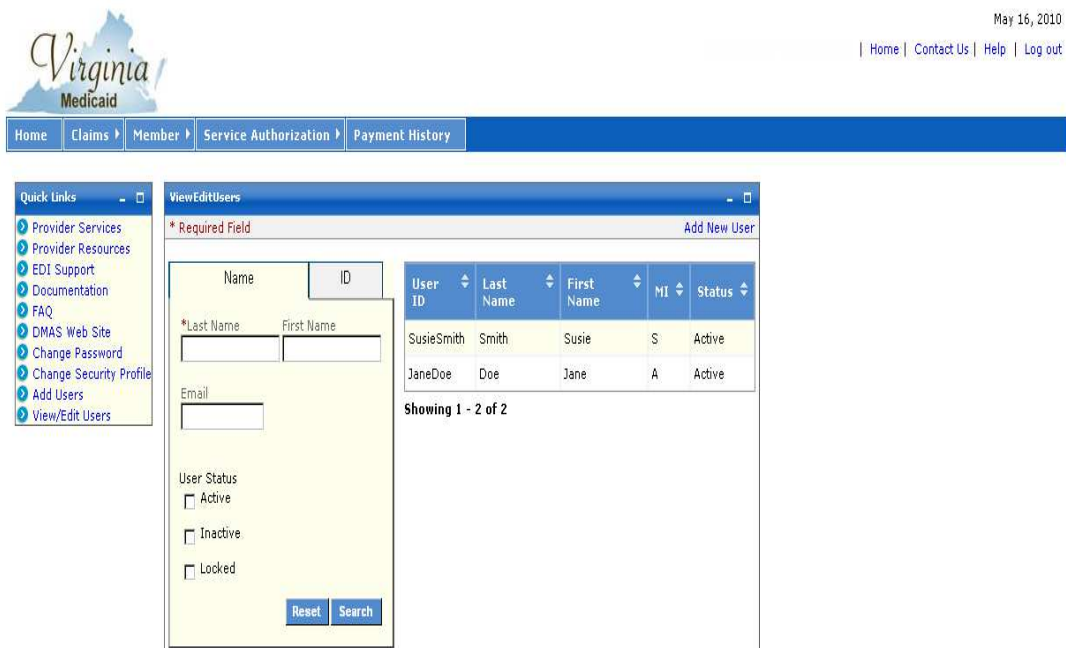
6.2 User List

The View/Edit Users page contains the list of users associated with the Primary Account Holder. The Primary Account Holder will see any Organization Administrators and Authorized Users (all three types).

The Organization Administrator will see any Authorized Users (all three types).

The user list will see the user's User ID, Last Name, First Name, Middle Initial and the user's status (i.e. Active, Inactive).

To update or modify a specific user, click on that user to retrieve their record.

The individual user record reflects the following information associated with the user:

- User ID
- User Status – Active or Inactive
- NPI – NPI or API the user is associated to
- Last Login – the date the user last logged in
- Password Expires – the date the user's current password expires
- User Name – Prefix, Last Name, First Name, Middle Initial & Suffix
- Phone Number/Extension – User's phone number & extension
- Email – User's email address
- Role – User's selected role

View / Edit User

Please enter the following information about the user you would like to edit.

User ID: JaneDoe

User Status: Active

NPI: 0015209906

Last Login:

Password Expires: 08/30/2011

Prefix	* Last Name	* First Name	MI	Suffix
▼	Doe	Jane		▼

* Phone / Ext   * Email

8045551212   jane.doe@acs-inc.com

* What roles will this user have in the organization?

Available   **Selected**

AuthorizedStaff   ->>   OrganizationAdministrator
AuthorizedStaff - Claims
AuthorizedStaff - Provider   ->

                              <-

                              <<-

[Cancel] [Reset] [Deactivate] [Reset Password] [Save]

6.3 Searching for a Specific User

For larger organizations, there may be too many members for the list and it might be easier to search for a specific user.

There are two mechanisms to search for a specific user.
- Name
- ID

6.3.1 Searching for a Specific User – Name Search

To search by a User's Name, enter the required and/or optional fields:

- **Last Name** * (required) – enter a full or partial last name to conduct the search on
- **First Name** (optional) – enter a full or partial first name to conduct the search on
- **Email** (optional) – enter a email address
- **User Status** (optional) – select any additional selection criteria

If only one record meets the search criteria the individual record will be presented. If multiple records meet the search criteria the list of matches will be displayed in the User List. You will need to select one of the users and the individual record will be presented.

6.3.2 Searching for a Specific User – ID Search
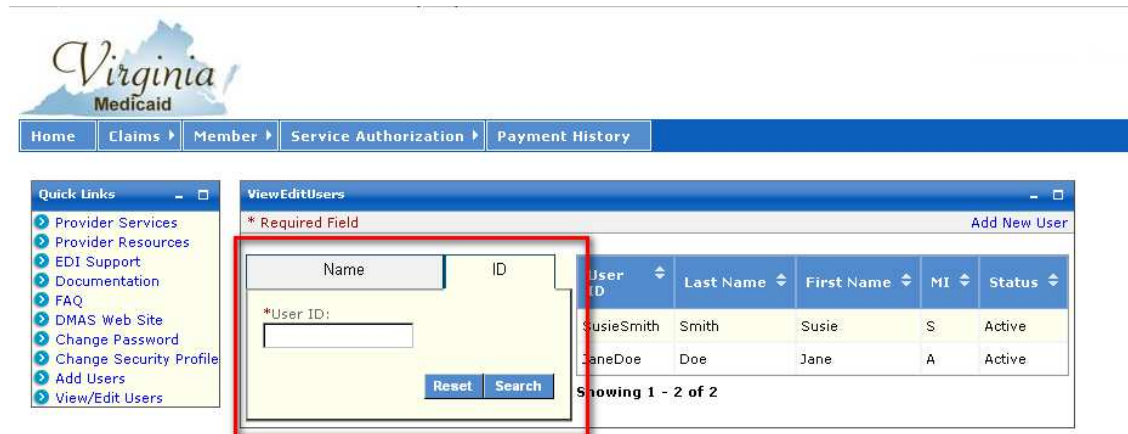
To search by a User's ID, enter a full or partial User ID to conduct the search.

If only one record meets the search criteria the individual record will be presented. If multiple records meet the search criteria the list of matches will be displayed in the User List. You will need to select one of the users and the individual record will be presented.

6.4 Changing a User's Role

To change a user's role within the provider organization, select the desired user record from the User List or conduct a Name or ID search.

Once the user record is selected, choose the role from the 'Available' column to move to the 'Selected' column and trigger the move with the -> arrow.

ViewEditUsers — □

* Required Field

View / Edit User

Please enter the following information about the user you would like to edit.

User ID: SusieSmith

User Status: Active

NPI: 0015209906

Last Login:

Password Expires: 08/30/2011

Prefix	* Last Name	* First Name	MI	Suffix
▾	Smith	Susie		▾

* Phone / Ext		* Email
8045551212		susie.smith@acs-inc.com

* What roles will this user have in the organization?

Available		Selected
AuthorizedStaff	->>	AuthorizedStaff - Claims
	->	AuthorizedStaff - Provider
	<-	OrganizationAdministrator
	<<-	

[Cancel] [Reset] [Deactivate] [Reset Password] [Save]

If a 'Selected' role needs to be de-selected, highlight the role to be moved back to 'Available' and trigger the move with the <- arrow.

View / Edit User

Please enter the following information about the user you would like to edit.

User ID: SusieSmith

User Status: Active

NPI: 0015209906

Last Login:

Password Expires: 08/30/2011

Prefix	* Last Name	* First Name	MI	Suffix
▼	Smith	Susie		▼

* Phone / Ext		* Email
8045551212		susie.smith@acs-inc.com

* What roles will this user have in the organization?

Available		Selected
AuthorizedStaff AuthorizedStaff - Claims AuthorizedStaff - Provider	->> -> <- <<-	OrganizationAdministrator

[Cancel] [Reset] [Deactivate] [Reset Password] [Save]

6.5 Resetting a Password

To reset a password, select the desired user record from the User List or conduct a Name or ID search.

Click on the 'Reset Password' button on the bottom of the page.

The 'Reset Password' screen below contains the selected user's information.

As the Primary Account Holder or the Organization Administrator, you need to enter a 'New Password' and 'Confirm New Password', as well as note the reason for the temporary password.

After completing the temporary password information, select 'Save'

View / Edit User

Please enter the following information about the user you would like to edit.

The password of User - SusieSmith has been reset to a One Time password successfully. The User can use this password to login at which time he/she must change it to a password of his/her choosing.

User ID: SusieSmith

User Status: Active

NPI: 0015209906

Last Login:

Password Expires: 08/30/2011

Prefix	* Last Name	* First Name	MI	Suffix
	Smith	Susie		

* Phone / Ext		* Email
8045551212		susie.smith@acs-inc.com

* What roles will this user have in the organization?

Available		Selected
AuthorizedStaff AuthorizedStaff - Claims AuthorizedStaff - Provider	->> -> <- <<-	OrganizationAdministrator

Cancel Reset Deactivate Reset Password Save

6.6 Activating/Deactivating a User

To deactivate or activate a user, select the desired user record from the User List or conduct a Name or ID search.

Click on the 'Deactivate' button on the bottom of the page. If the user had previously been deactivated, this button will say 'Activate'

The 'Deactivate' screen below contains the selected user's information.

As the Primary Account Holder or the Organization Administrator, you need to enter a note as to the reason for the deactivation (or reactivation).

Click on 'Deactivate' to process the request.

6.7 Unlocking a User's ID

To unlock a user's id, select the desired user record from the User List or conduct a Name or ID search.

If a user has locked their account, an 'Unlock' button will show up on the bottom of the page.

Clicking on the 'Unlock' button will route you to the 'Unlock User' page.

Complete the reason for the unlocking and click on the 'Unlock' button.

If the unlocking was successful, an appropriate message will be displayed.

Appendix A – Glossary of Terms

Term	Definition
API	Atypical Provider Identifier – assigned by the Commonwealth of Virginia for providers that are not eligible for an NPI (i.e. transportation providers).
Authorized User	The staff that is responsible for performing provider support functions.
Authorized User – Claims	The staff that is responsible for Claims Direct Data Entry as well as performing provider support functions.
Authorized User – Provider	The staff that is responsible for updating provider demographics as well as performing provider support functions.
Automated Response System (ARS)	The Web Portal system that gives provider organizations access to provider support functionality such as Member Eligibility Inquiries, Service Limit Inquiries, Claims Status Inquiries, etc.
Claims Direct Data Entry (DDE)	The Web Portal system that allows provider organizations to create claims templates and/or submit professional and institutional claims.
Navigational Tabs	Tabs on a portal page that will take the user to other sections in the portal or bring up documents.
NPI	National Provider Identifier
Organization Administrator (OrgAdmin)	The person(s) who can also establish the Authorized User role and can reset the passwords, activate and deactivate users and lock and unlock user IDs for Authorized Users.
Portlets	Sections or 'boxes' that comprise a web portal page
Primary Account Holder	The person who will perform the initial web registration and will establish the security needed to allow the access to secured provider functionality
Provider Profile Maintenance	The Web Portal system that allows provider organizations to update designated demographic information.
Provider Organization	Either an individual provider or group provider and the user community in support of them.
User	Any person that will access the Web Portal and leverage the functionality within it.

Appendix B – Registration FAQ

<div style="background-color: navy; color: white; text-align: center;">

Virginia Medicaid Web Portal
Web Registration
Frequently Asked Questions
Revised 08/11/2015

</div>

<div style="background-color: blue; color: white; text-align: center;">

General Questions

</div>

How do I access the new Virginia Medicaid Web Portal?

The new Virginia Medicaid Web Portal can be accessed through the following link:
www.virginiamedicaid.dmas.virginia.gov

If I forget my password then who should I contact to have my password reset?

On the Virginia Medicaid Web Portal – Provider Login Page there is a 'Login' portlet. At the bottom of that portlet, click on the link labeled "Forgot My Password". The link will direct you to the three security questions submitted during the creation of your Security Profile. (See 'Establishing a Security Profile' FAQ Section).   You will be required to answer all three security questions correctly. Enter your User ID then select continue. Your password will be emailed to the email address in your user profile; the email address entered when registering. (See 'Establishing a User Profile' FAQ Section – Completing the User Profile').

If I forget my User ID what do I need to do to retrieve my User ID?

On the Virginia Medicaid Web Portal – Provider Login Page there is a 'Login' portlet. At the bottom of that portlet, click on the link labeled "Forgot User Name". The link will direct you to the three security questions submitted during the creation of your Security Profile. (See 'Establishing a Security Profile' FAQ Section).   You will be required to answer all three security questions correctly. Enter your Email Address (previously entered in your profile when you registered, then select continue. Your User ID will be emailed to your email address. (See 'Establishing a User Profile' FAQ Section – Completing the User Profile').

Getting Started

First Time Users

I'm an enrolled provider, or user associated to an enrolled provider, who has never registered with the Virginia Medicaid Web Portal. What is involved in the registration process?

To take advantage of the portal, your designated Primary Account Holder, will need to register and request secured access. Requesting secured access is used to authenticate you as the provider or Primary Account Holder.

As a new user you will need to complete the following steps:

1. Establish a User ID, Password and security profile
2. Request secured access for your organization
3. Successfully complete a one-time verification process of 3 questions
4. Upon receipt of confirmation email, click link within email
5. Sign in to the secured portal

As a user trying to register with the Virginia Medicaid Web Portal, how do I start?

To begin the registration process, please access the portal at www.virginiamedicaid.dmas.virginia.gov .

On the portal home page select 'Provider' from the Login portlet. You'll be directed to the Provider Login page where you'll see the 'First Time User Registration' portlet. Click on 'Register' to begin the registration process. You can also access the registration process via the 'First Time User?' link in the Login portlet.

As part of this process, you'll be directed through the creation of a user and security profile. The user profile will help you to create a User ID and password. See 'Establishing a User Profile' FAQ Section.

 The Security Profile will request the completion of three (3) questions. These will be needed in order to assist you should you forget your User ID or password in the future. See 'Establishing a Security Profile' FAQ Section – 'Creating Security Questions'.

After completing your profile, if you are the designated Primary Account Holder, you may request secured access for the NPI organization.

Requesting secured access will initiate the authentication process and establish your access to your secured provider functions. See 'Establishing a Security Profile' FAQ Section – 'Requesting Secured Access'.

You will also be able to leverage the portal to establish a user organization, enabling the addition of Organization Administrators and Authorized Staff as needed to support your organizational needs. See 'Establishing a User Organization' FAQ Section

How is my User ID assigned?

For the first time portal user, the User ID is determined and entered by the user at the time of registration, in conformance with the User ID criteria. (See 'Establishing a User Profile' FAQ Section – 'Creating a User ID')

How is my password assigned?

For the first time portal user the password is determined and entered by the user at the time of registration, in conformance with the password criteria. (See 'Establishing a User Profile' FAQ Section – 'Creating a Password')

I have to complete a User Profile and establish a Security Profile. What are these and why do I need them?

The User Profile is part of the registration process and contains the following information. Any information that is required (noted with an asterisk *) will need to be supplied by you at the initial login.

- Associated NPI
- User ID *
- NPI's FEIN
- Password *
- First Name *
- Middle Initial
- Last Name *
- Phone Number *
- Extension
- Preferred email *

The Security Profile contains three (3) security questions. Completion of three questions is required. This information is used in assistance with forgotten User IDs or passwords.

For more information, please see 'Establishing A User Profile' and 'Establishing a Security Profile' FAQ Sections

I'm a designated Primary Account Holder for my provider organization. I need to request secured access in order to complete my authentication process and gain access to secured provider functionality. What is 'secured access'?

Requesting secured access is a mechanism for authenticating the Primary Account Holder with the associated provider.

To initiate the authentication process, you will complete the registration and then Request Secured Access. See 'Establishing a Security Profile' FAQ Section – 'Request Secured Access'

Upon successful authentication, an email will be sent to the Primary Account Holder. Once received, you will click the included link to complete the authentication. See 'Establishing a Security Profile' FAQ Section – 'Request Secured Access'

Once validated you will have access to secured provider functionality such as:
Claims – Claims Status Inquiry and Claims Direct Data Entry options
Member – Member Eligibility, Member CoPay and Member Service Limits

Service Authorization – Service Authorization Log
Payment History – Provider Payments
EHR Incentive Program – Information and Links associated with the EHR Incentive Program
Provider Maintenance – Provider Demographic Maintenance, Disclosure, Revalidations and Revalidation Status Tracking.
Provider Enrollment – Online applications for provider enrollment
RA Messages – RA messages available for providers receiving electronic remittances.
Level of Care Review - Level of Care Review Instruments
Pre-Admission Screening – Pre-Admission Screening forms, Status Tracking, File Upload and Assessment Search

I'm a designated Primary Account Holder for my provider organization. How do I establish my user organization?

The Primary Account Holder will be able to establish the provider organization, setting users up as either Organization Administrators or Authorized Staff. Organization Administrators will be able to set up Authorized Staff.

See 'Establishing a User Organization' FAQ Section for more details.

Establishing a User Profile

Creating a User ID

Is a User ID required for initial registration on the Web Portal?

Yes, you must create a User ID to log in to the Web Portal.

How do I get a User ID?

For an already established organization, the Primary Account Holder and OrgAdmin for your organization have the authority to establish User IDs.

For a designated Primary Account Holder, you will need to create your User ID at the time of initial registration.

What are the criteria for creating a User ID?

The User ID must be a minimum of 6 characters and a maximum of 16 characters. It can include hyphens, underscores or periods. The User ID can not start with special characters nor can it contain spaces.

Creating a Password

How was my password assigned?

If you're the designed Primary Account Holder for your provider organization, the first time you access the portal, you will create the password in conformance with the password criteria.

If you're not the designated Primary Account Holder for your organization, you will need to get your initial password from your Primary Account Holder or Organization Administrator. Upon your initial access to the portal, you will be immediately directed to change your password.

What are the criteria for creating a password?

The portal password must be a minimum of 8 characters and must include three (3) of the following four (4) requirements:

- Capital/Upper case letter
- Lower case letter
- Number
- Special character (!, $, #, %)

How often will I be required to change my password?

Passwords will need to be changed every 42 days.

Completing the User Profile

I have to complete a User Profile and establish a Security Profile. What are these and why do I need them?

The User Profile is part of the registration process and contains the following information. Any information that is required (noted with an asterisk *) will need to be supplied by you at the initial login.

- Associated NPI
- User ID *
- NPI's FEIN
- Password *
- First Name *
- Middle Initial
- Last Name *
- Phone Number *
- Extension
- Preferred email *

The Security Profile contains three (3) security questions. Completion of three questions is required. This information is used in assistance with forgotten User IDs or passwords.

For more information, please see 'Establishing a Security Profile' FAQ Sections.

Do I need a NPI or a API to register?

No, a NPI or API is not required at the time of initial registration. An API or NPI is required at the time secured access is requested. If the NPI/API is known at the time of registration, it is recommended that it be entered at that time.

What is the maximum length of the characters allowed for my first name?

The maximum number of characters allowed is 25.

Is the first name field required for registration to the Web Portal?

Yes, this is a required field.

What is the maximum length of the characters allowed for my last name?

The maximum number of characters allowed is 25.

Is the last name field required for registration to the Web Portal?

Yes, this is a required field.

What format do I use to enter the telephone number?

You must enter 10 digits (area code and phone number) with no spaces or hyphens.

Do I have to have an email address to register?

Yes, an email address is required. The email address is utilized to send users temporary passwords and to send users their forgotten User IDs. For the Primary Account Holder, the email address is used in the completion of the authentication process.

Establishing a Security Profile

Creating Security Questions

There are three security questions listed in the Security Profile. Do I need to pick a question from each security drop down list?

Yes, you need to choose a security question from each of the three columns. The same questions appear in each security question drop down. You are required to pick one question from each security question drop down for a total of three questions. You may not choose the same question previously chosen in another security question.

These security questions will be utilized in assisting you with a forgotten User ID or password.

Request Secured Access

Why do I need to Request Secured Access?

As the designated Primary Account Holder for your organization, you will need to initiate and complete the authentication process. Requesting secured access is a one-time process to be completed only by the Primary Account Holder.

Do all users need to request secured access?

No, requesting secured access is a one-time process needed only to authenticate the Primary Account Holder to the provider.

How do I Request Secured Access?

To Request Secured Access, complete the initial registration process. From the Provider Welcome page there are two options for requesting secured access. On the Quick Links to the left is a link to 'Request Secured Access'. In the Welcome verbiage, Step 2 also contains the link to 'Request Secured Access.'

Clicking this link will trigger the authentication process.

How do I complete the authentication process?

The PAH will be required to complete three questions. The first question will require either the provider's SSN or FEIN. Drop down options will be based on what information is captured in the MMIS.

Validation Question 1 could contain the following drop down values:

- Provider's SSN (last 4 digits)
- Provider's FEIN (last 4 digits)

Validation Questions 2 and 3 will contain a list of provider information available on the MMIS. The user can select any question available in the drop down. Question 2 and 3 must be different though.

Possible Question options (unless the information is not on the MMIS for the provider secured access is being requested for):

- License End Year (YYYY)
- Provider's birth year (YYYY)
- Zip Code of Provider's Correspondence Address
- Bank Routing Number (last 4 digits)
- Bank Account (last 4 digits)
- EDI Submitter ID

If validation is unsuccessful, you will receive the following error message:

The secured access for your provider organization has not been validated. Question(s) <<1, 2, 3>> has/have been answered incorrectly. Please correct your answers or contact the provider for information to correctly complete. If you have any additional questions, please contact the Web Portal support help desk at 866-352-0496.

Upon successful authentication of the questions entered, you will receive the following error message:

The secured access for your provider organization has been validated. You will receive an email shortly with instructions for finalizing the authentication process or you can log off now and log back on to trigger your updated access.

I've successfully completed the authentication process. Where is the email sent?

A Secured Access Confirmation will be sent via email to the Primary Account Holder's email address.

Upon receipt, the PAH will need to click the link within the email. Signing in to the web portal will activate the secured access for you and the rest of the provider's organization.

Note: The purpose of the email is to ensure you log off and log on again after registration is complete. This will initiate the secured access. You can do this without waiting for the email if you wish.

You should now see all secured functionality (i.e. Claims Status, Member Eligibility, etc.). If not, please contact the Web Portal Support help desk at 866-352-0496.

If you haven't done so already, you can begin/continue creating (or modifying) your user organization. Click 'Add New Users' or 'View/Edit Users' from the Quick Links on the left side of the portal page. For more complete instructions, please refer to FAQ section 'Establishing a User Organization'.

Establishing a User Organization

Security Roles

What roles are part of the new Virginia Medicaid Web Portal?

The new Virginia Medicaid Portal has three (3) security roles currently established.

- Primary Account Holder
- Organization Administrator (OrgAdmin)
- Authorized Staff roles:
  - o Authorized Staff
  - o Authorized Staff – Claims
  - o Authorized Staff - Provider

What is a Primary Account Holder?

A Primary Account Holder is the person who will perform the initial web registration. He/she will establish the security needed to allow the access to secured provider functionality (i.e. ARS functions, Claims DDE or Provider Maintenance). The Primary Account Holder can also establish the Organization Administrator (OrgAdmin) and Authorized User roles. The Primary Account Holder can reset the passwords, lock and unlock users for OrgAdmins or Authorized Users.

What do we do if our Primary Account Holder is no longer associated with our organization?

If your Primary Account Holder is no longer associated at your Organization or has moved to another department please contact the Virginia Medicaid Help Desk. For Help Desk information, click on the Contact Us link placed at the right corner of the Provider log in page.

How do we change our Primary Account Holder?

Any change to the Primary Account Holder (PAH) must be made in writing by completing and faxing the Primary Account Holder Change Form into the Virginia Medicaid Web Support Helpdesk. The Primary Account Holder Change form and instructions for completing can be found under Web Registration Reference Material.

What is an Organization Administrator?

The OrgAdmin can also establish the Authorized User role. He/she can reset the passwords, lock and unlock User IDs for Authorized Users.

Who can be set up as an OrgAdmin?

The Primary Account Holder can establish the OrgAdmin role for an organization.

What is an Authorized Staff?

Within the Authorized Staff category there are three distinct functions:
• Authorized Staff
• Authorized Staff – Claims
• Authorized Staff – Provider

All three roles apply to staff that is responsible for performing Automated Response System (ARS) functions such as Member Eligibility Inquiries, Service Limit Inquiries, Claims Status Inquiries, etc.

Authorized Staff – Claims has the additional capability of being able to submit claims via the Claims Direct Data Entry system on the Web Portal.

Authorized Staff – Provider has the additional capability of being able to update provider demographic information via the Provider Profile Maintenance system on the Web Portal.

Adding and Modifying Users

Who can add or modify users for my organization?

Only Primary Account Holders can add Organization Administrators. Both Primary Account Holders and Organization Administrators can add Authorized Staff.

How do I add a user?

To add a user to your organization, from the Provider Welcome page, click on 'Add User' from the Quick Links on the left.

Establish a User ID for the staff member. The User ID must conform to the User ID requirements. See 'Establishing a User Profile' FAQ Section – 'Creating a User ID' for User ID requirements.

Complete the following required user information:
• Last Name
• First Name
• Phone Number
• Email

Establish a temporary password for the staff member. The password must conform to the password requirements. See 'Establishing a User Profile' FAQ Section – 'Creating a Password' for password requirements.

Choose the user's role within the organization. Your role will determine what available roles are displayed. A Primary Account Holder will see both Authorized Staff and Organization Administrator options where an OrgAdmin will only see Authorized Staff as a role.

Note: The User ID and Password created during this process will NOT be emailed to the new user. The Primary Account Holder must provide the staff member with the User ID and Password created.

How do I modify a previously established user?

To modify a user's information, including resetting their password, changing a user's role, deactivating or activating a user or unlocking a user who's exceeded their log in tries.

From the Provider Welcome page, click on 'View/Edit User' from the Quick Links on the left. Select desired user from list or search for the desired user based on User ID or name.

If I want to change role assignments, do I just call the Virginia Medicaid Help Desk?

There are several ways to learn how to change role assignments.

• Self- Help Methods
  o Web Registration Tutorial
  o Web Registration User Guide
  o Web Registration Quick Reference Guide

All of these can be located on the portal under the Provider Resources tab – Web Registration Reference Material link

- Contact the Virginia Medicaid Help Desk

If you have the necessary authority to make the change, the Virginia Medicaid Help Desk will take the user through the role modification procedure.

 If you do not have the necessary role authority to make the change, Xerox will not make any role changes without written authorization from the provider entity authorizing the change.

Xerox will retain this authorization for audit purposes. Please submit written authorization to Xerox via mail (USPS), email or fax to Xerox.