



## **Obtaining Access to CIMOR, Consumer Referral Database, Mortality Review and File Transfer Protocol for DD Service Providers January 2016**

### **CONTENT:**

- PART I: Page 2: Essential information for CIMOR users.**
- PART II: Page 2: New Provider Contract: Establishing a Local Security Coordinator/Officer (LSO) after contract is in place.**
- PART III: Page 4: Granting additional employee's access to CIMOR once the contract and LSO have been established.**
- PART IV: Page 5: Requesting CIMOR roles through Access Request Application (ARA) – All staff**
- PART V: Page 9: Tracking ARA Requests and List of Current Roles**
- PART VI: Page 10: Requesting Entry or Changes to DD Provider Rep in CIMOR as relates to Health Inventories (residential providers only).**
- PART VII: Page 11: Revoking User Access**
- PART VIII: Page 11: CIMOR Billing Training**
- PART IX: Page 11: Password Requirements**
- PART X: Page 12: Changing Your Password**
- PART XI: Page 13: Accessing Providers File Transfer Protocol**

## **PART I: Essential information for CIMOR users.**

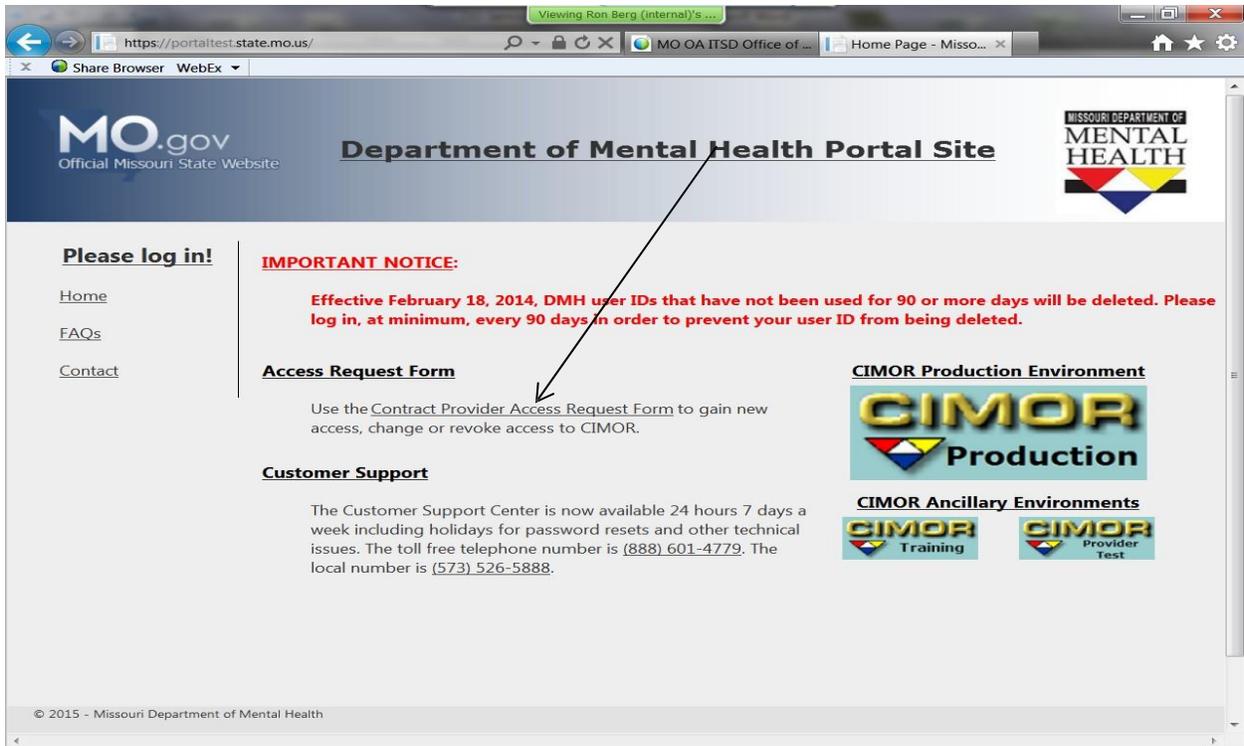
- When you obtain a User ID and Password, log onto the DMH Portal Website (<https://portal.dmh.mo.gov/>) and change your password prior to any further action. If you skip this step, you must call the helpdesk and reset your password.
- Your password is only good for 60 days. You will not receive any reminders.
  - **This is the #1 reason why users are not able to access CIMOR.**
  - If you forget to change your password in a timely manner or enter an incorrect password too many times (3 or 4) you will be locked out of your account.
  - If you try to sign on and receive the message “invalid user credentials” or “contact your local security officer” this is usually related to a password no longer being valid.
  - If this happens, contact Customer Support Center at 573-526-5888 or toll free at 888-601-4779. A technician will respond to your request within 2 hours of receiving the request.
- DMH user IDs that have not been used for 90 or more days will be deleted. Please sign on a minimum of every 90 days in order to keep your user ID from being deleted. The user will have to resubmit a Contract Provider Access Form and go through the ARA process again if the ID is deleted.
- Local Security Officer (LSO) needs to maintain access to CIMOR at least 1x every 60 days and update email address if it changes (update in Profile at top of portal.) LSO has to approve other user’s access request after receipt of notification through the email system. If email is not current, LSO will not receive notification.
- When an email is sent to the Local Security Coordinator/Officer (LSO) only the LSO should respond to that email.
  - Having someone else answer the email will result in loss of access to CIMOR due to a potential security breach. This will be extremely inconvenient if it occurs during billing periods.
- Do not share your user ID and Password. This will also result in loss of access to CIMOR due to a potential security breach.
- If an employee with access to CIMOR leaves the agency you need to IMMEDIATELY revoke their access. See Part VII.

## **PART II: New Provider Contract: Establishing a Local Security Coordinator/Officer (LSO) after contract is in place.**

The first part of the process requires submitting required documentation to obtain a User ID and password.

Step 1: Complete the Contract Provider Access Request Form at <https://portal.dmh.mo.gov/>

- Under Part 3, all residential providers need to indicate “add” to Mortality Review
- Under Part 4, all residential providers need to indicate “add” to Consumer Referral DB
- Under Additional Data Request, you may want at least one staff to indicate **FTP File**. If the LSO will be this staff or one of the staff, enter this information. See Section XI for information about FTP to help you decide if you want access and who should have access.



**Step 2:** Draft a letter with the below components onto provider letter head. Example:

Provider Name

Address

City, State Zip

Phone

Fax

Date

Attention: (Provider Relations Liaison), (Local Regional Office Name)

(Local Regional Office Address)

(Provider Relations Liaison):

RE: LSO and Provider Staff w/ Access to CIMOR

Our Local Security Officer (HIPAA) is: Name of Staff e-mail address

Sincerely,

Executive Director Signature

**Step 3:** Fax completed documents to your local Regional Office. They will forward to OA for Assignment.

OA will provide the LSO a user ID and password. You will receive this information back from your local regional office.

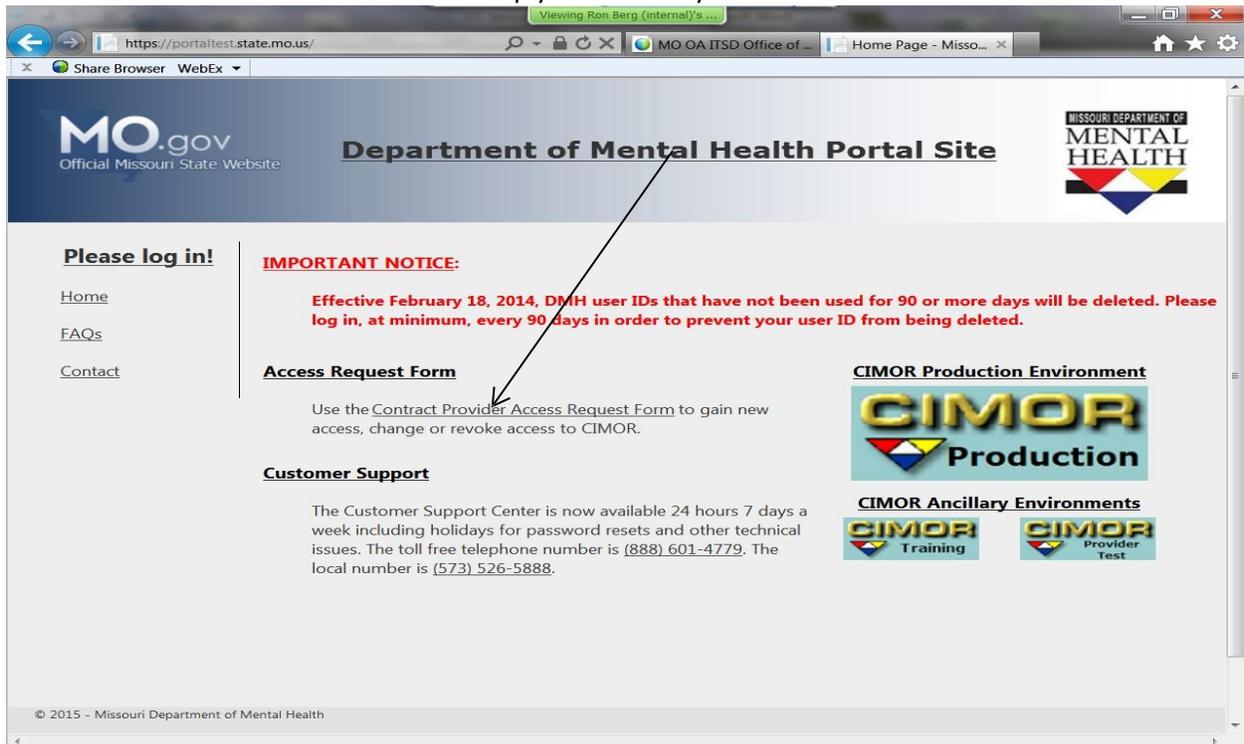
Once the LSO receives their new user ID and password, they need to log into the portal and change their password. See Part X for details on changing your password. Then proceed to Part IV to obtain CIMOR access by completing an ARA.

Note: if LSO leave the agency, immediately revoke and reassign a new LSO. The LSO grants additional provider employee's requests for access. Without an LSO identified, requests cannot be processed.

### **PART III: Granting additional provider employee's access to CIMOR once the contract and LSO have been established.**

Step 1: Complete the Contract Provider Access Request Form at <https://portal.dmh.mo.gov/>.

- Under Part 3, all residential providers need to indicate "add" to Mortality Review
- Under Part 4, all residential providers need to indicate "add" to Consumer Referral DB
- Under Additional Data Request, you may want at least one staff to indicate **FTP File**. See Section XI for information about FTP to help you decide if you want access and who should access.



Step 2: Fax completed document to your local Regional Office Provider Relations Liaison who will forward to OA.

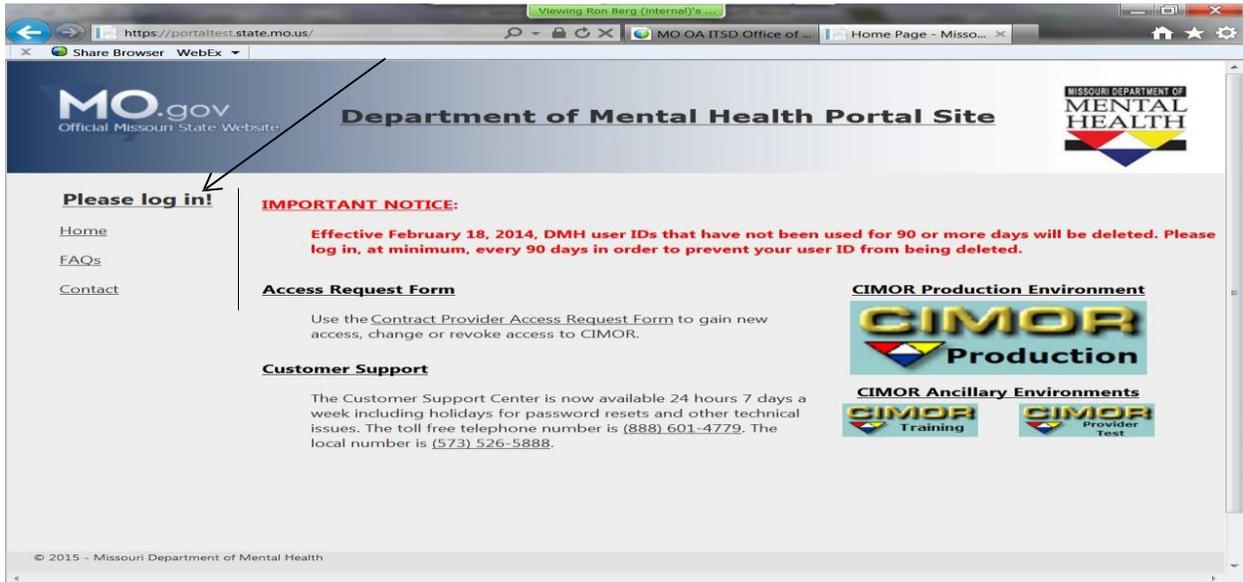
OA will provide the employee a user ID and password....you will receive this information from your local RO PR liaison.

Once the employee has received their user ID and password, they need to log into the portal and change their password. See Part X for details on changing your password. Then proceed to Part IV to obtain CIMOR access by completing an ARA.

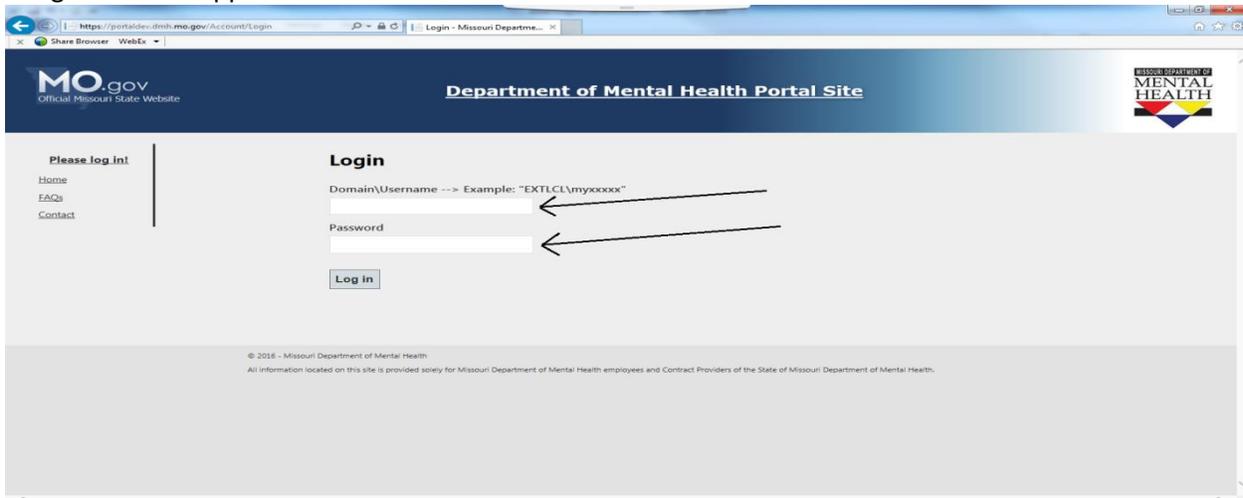
## PART IV: Completing an Access Request Application for CIMOR roles

Completing an Access Request Application (ARA) is necessary to add provider roles in CIMOR, such as billing access and Health Inventories (HI is required for residential providers.)

STEP 1: The user logs into the DMH Portal web site at <https://portal.dmh.mo.gov/>



A log-in box will appear.

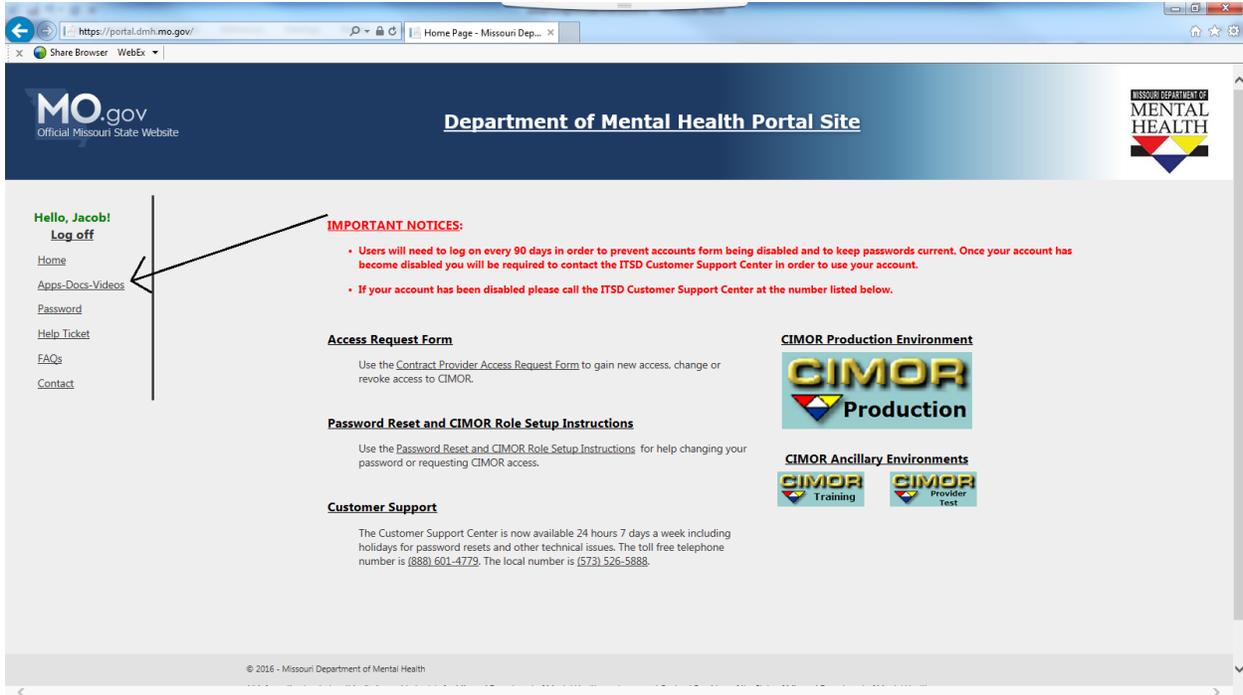


In the User name box, the user must enter their Domain Name, i.e. EXTLCL and a backslash \ (This is the slash mark above the Enter key). For example: extlcl\mytesta. Tab to the second box and enter the password.

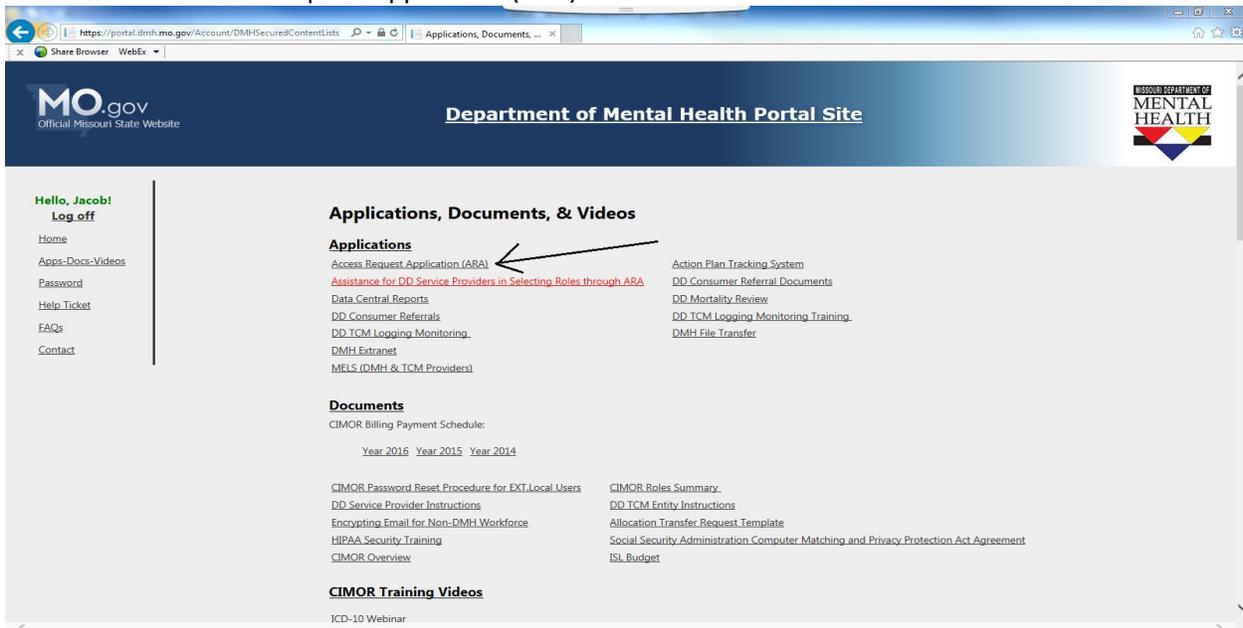
The main portal page will appear and acknowledge that you have logged on by saying "Hello, user name" in the upper right hand corner.

If you are a first time user or had the Help Desk change your password, you need to change your password before going further. See Part X for details on changing your password. Then pursue Step 2.

## STEP 2: Select Apps-Docs-Videos



## STEP 3: Select Access Request Application (ARA)



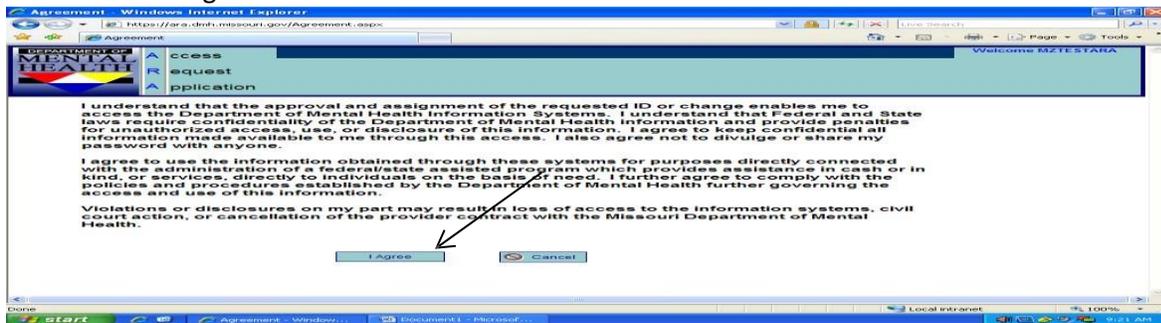
STEP 4: Enter User Name and Password. In the User name box, the user must enter their Domain Name, i.e. EXTLC and a backslash \ (This is the slash mark above the Enter key). For example: extlcl\mytesta. Tab to the second box and enter the password.

**STEP 5: Select New Request**



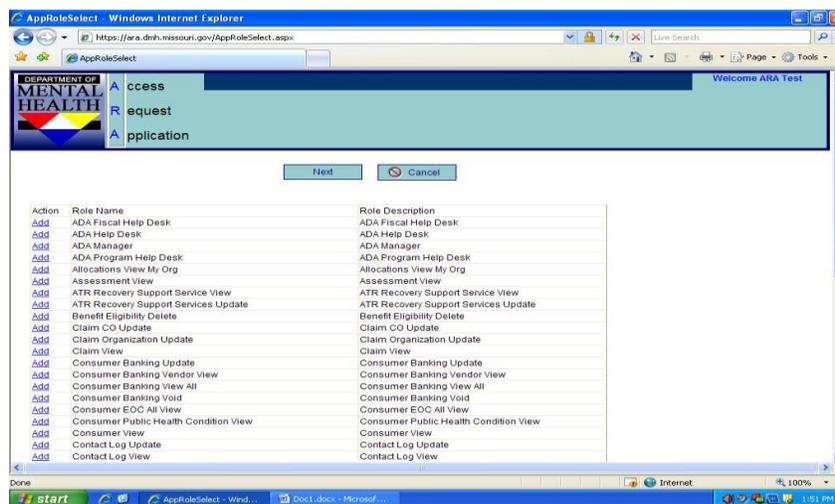
**STEP 6: Enter Email Address as prompted.**

**STEP 7: Click "I Agree"**



**STEP 8: In the next screen that appears, click the arrow in the Employer drop down to select your provider agency.**

In the next screen after choosing the provider's name for Employer, the list of CIMOR roles appears.



The user will click Add for each role they need to access, waiting for a role to highlight before selecting the next role.

**Note: Please refer to the CIMOR Security Roles Document available in the Apps-Docs-Videos Section for guidance in choosing roles. Not all roles are available for providers. If a request is submitted for a role a provider is unable to have, the entire request will be denied and a new request must be submitted. Review roles document to decide which ones you want each employee to have.**

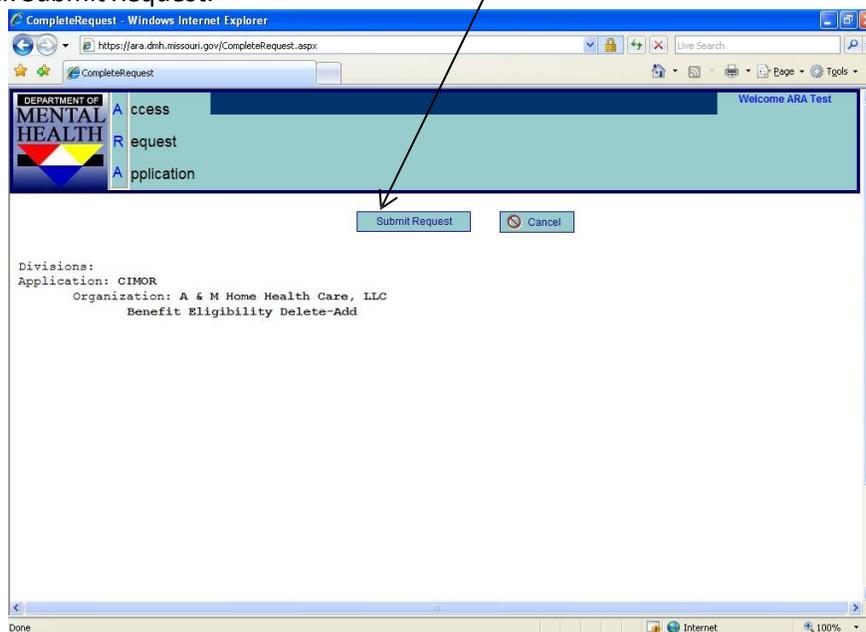
Typical Roles for DD Providers are:

- MR Provider Billing (for billing personnel or others to check)
- MR Provider Billing View Only (if you have an employee who needs to see billing but will not actually perform billing)
- DD Provider Profile Update (for employees who will be responsible for inputting and updating information related to the Division website Provider Profile Directory – a resource for individuals and family members \*)
- Division MRDD \*^
- DMH Invoice Org View (billing related, allows to search SAM invoices) \*^
- HIPS Nursing Review View (**residential providers** only) \*
- My Organization User \*^
- Screening View (**residential providers** in relation to HIPS NR)\*

\*These roles are included in the MR Provider Billing role. Only request if specific employee does not have/request the MR Provider Billing Role

^These roles are included the MR Provider Billing View role. Only request if specific employee does not have/request the MR Provider Billing View role.

Select “Add” next to the first role and wait for the role to be highlighted, then select the next role and wait for highlight and so on. **After selecting the necessary roles, the user will click Next at the top of the screen.** A review screen appears. Please review the selected roles and make any corrections if necessary. Click Submit Request.



A screen will appear indicating the request has been submitted.

The request will electronically route to the provider Local Security Officer (LSO) to the email address on file with DMH. After the LSO has approved roles by clicking on the link and signing with their user id and password, the ARA will route electronically to the Department of Mental Health for final approval.

If roles have been selected correctly and the LSO has approved, CIMOR access is granted within 48 hours. If, however, any roles have been chosen that are not available to providers, the ARA will be denied and the user and Local Security Officer will receive an e-mail indicating why the request was denied. The request will then need to be resubmitted for approvals.

## PART V: Tracking ARA Requests and List of Current Roles

### 1. Tracking ARA Requests

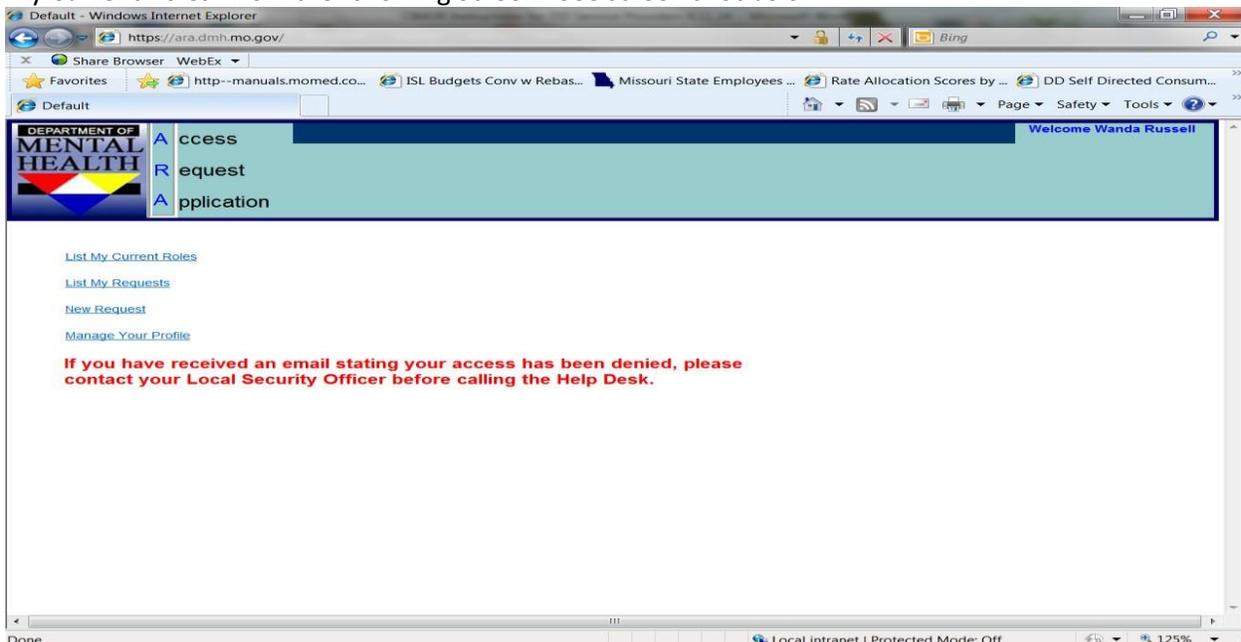
After an ARA has been submitted, the employee can track where the request is in the process.

The User should log onto the portal and select “Access Request Application (ARA)” from Docs – Forms as in Part IV Step 3. Select “List My Requests” from the following Screen. See screen shot below.

### 2. Obtaining a list of current approved roles or access.

At any time, an employee can review the roles or accesses in CIMOR that they have been granted.

Log onto portal and select “Access Request Application (ARA)” from Apps-Docs-Videos. Select “List My Current Roles” from the following Screen. See screen shot below.



## **PART VI: Requesting Entry or Changes to DD Provider Rep in CIMOR as relates to Health Inventories (residential providers only).**

A DD Provider Rep should be named for each consumer in your residential services. This will be the person who will receive an automated email when a Nurse Review has been completed or modified. There can only be one DD Provider Rep named at a time however see Step 2.d below for an option.

### Steps

1. Residential Providers who need their DD Provider Representative updated in CIMOR for their consumers will submit all requests to:

Janet Leonard: [Janet.Leonard@dmh.mo.gov](mailto:Janet.Leonard@dmh.mo.gov)

2. Information to be submitted:
  - a. Staff Name who is named DD Provider Representative and for which individual or individuals. You can also indicate the same person/ email for all consumers in your agency.
  - b. The DD Provider Representative email address.
  - c. Include start dates or end dates as applicable to request having someone added or removed from CIMOR DD Provider Rep.
  - d. For larger organizations, consider creating a “group” email name and address to submit as your DD Provider Rep. This will allow the email notification that a Nurse Review has been completed go to all who are attached to that address. This will also allow the DD Residential Provider the ability to manage that group email list w/o having Ann change this in CIMOR for you each time. These individuals will then need to have the proper role access in CIMOR to see the Nurse Review.

## **PART VII: Revoking User Access**

When an employee who has access to CIMOR leaves an agency:

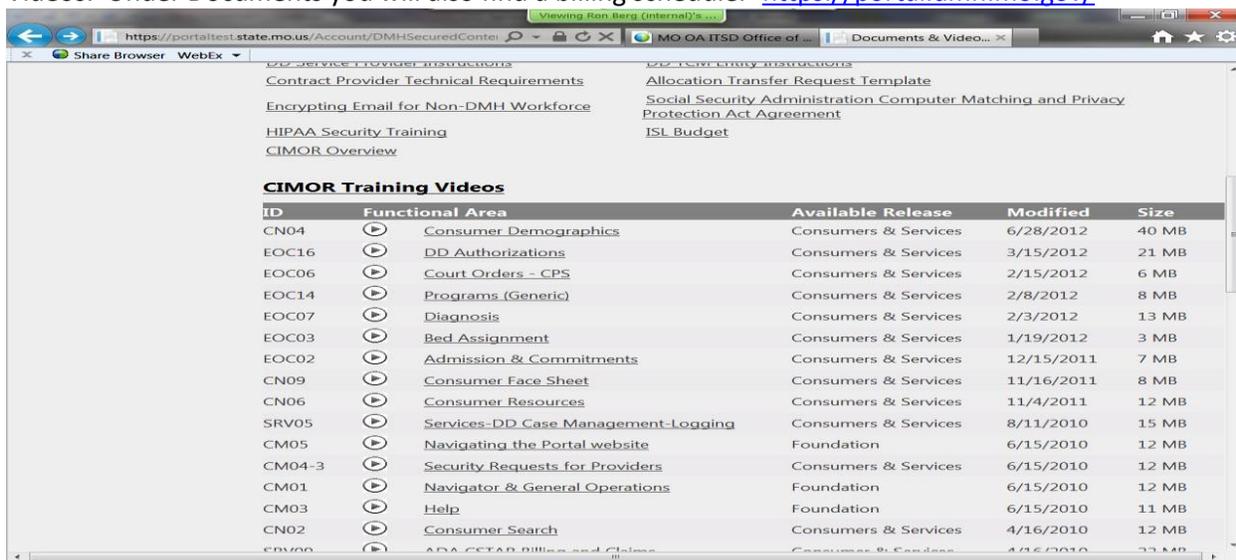
- IMMEDIATELY submit the **Contract Provider Access Request Form** found on the home page of the portal, indicating “Revoke” and the employee’s name. Fax the form to your local Regional Office Provider Relations liaison for processing.
- Remember, if the employee was a DD Provider Representative for the Health Inventory process, you will need to follow the directions in Part IV to assign a new DD Provider Representative.
- If the employee is the LSO, the provider will need to identify a new LSO by completing Steps 1 and 2 in Part 1 in addition to revoking access to the previous LSO.

Revoking user access is essential to an agency for security purposes. The ex-employee is able to access CIMOR from any location as long as they still have access approval.

**As the person is no longer employed, it is a violation of confidentiality to have access to consumer information. The person's access could create errors in billing information.**

## PART VIII: CIMOR Billing Training

Once your billing staff receives access approval, they should log into same portal and select Apps-Docs-Videos from the list on the left side of the screen, and scroll down to find/review CIMOR Training Videos. Under Documents you will also find a billing schedule. <https://portal.dmh.mo.gov/>



ID	Functional Area	Available Release	Modified	Size
CN04	Consumer Demographics	Consumers & Services	6/28/2012	40 MB
EOC16	DD Authorizations	Consumers & Services	3/15/2012	21 MB
EOC06	Court Orders - CPS	Consumers & Services	2/15/2012	6 MB
EOC14	Programs (Generic)	Consumers & Services	2/8/2012	8 MB
EOC07	Diagnosis	Consumers & Services	2/3/2012	13 MB
EOC03	Bed Assignment	Consumers & Services	1/19/2012	3 MB
EOC02	Admission & Commitments	Consumers & Services	12/15/2011	7 MB
CN09	Consumer Face Sheet	Consumers & Services	11/16/2011	8 MB
CN06	Consumer Resources	Consumers & Services	11/4/2011	12 MB
SRV05	Services-DD Case Management-Logging	Consumers & Services	8/11/2010	15 MB
CM05	Navigating the Portal website	Foundation	6/15/2010	12 MB
CM04-3	Security Requests for Providers	Consumers & Services	6/15/2010	12 MB
CM01	Navigator & General Operations	Foundation	6/15/2010	12 MB
CM03	Help	Foundation	6/15/2010	11 MB
CN02	Consumer Search	Consumers & Services	4/16/2010	12 MB
CM00	ADA/CFRAB Billing and Claims	Consumers & Services	4/16/2010	12 MB

## PART IX: Password Requirements

Your new password must be at least 8 characters in length.

You must change your password as soon as you receive your first temporary password, immediately after having the help desk reset your password, and prior to your password expiring.

Your password will expire every 60 days.

You cannot reuse your last 24 passwords.

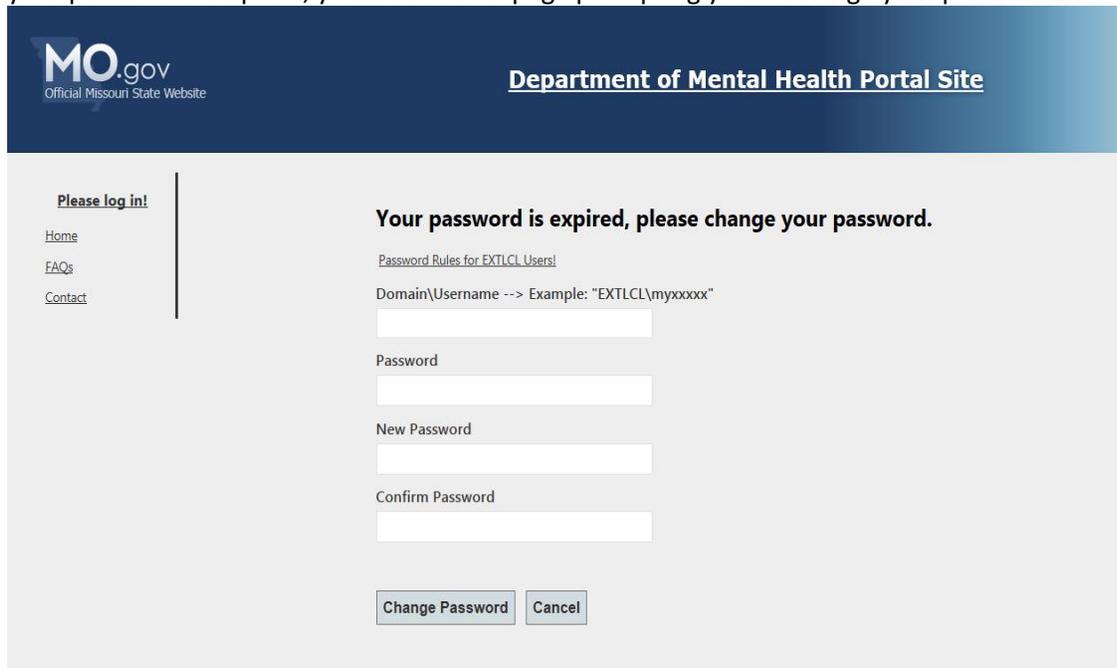
Your new password must contain at least 3 of the following 4 character groups:

- 1) English uppercase (A through Z)
- 2) English lowercase (a through z)
- 3) Numerals (0 through 9)
- 4) Non-alphabetic (such as !, \$, #, %)

## PART X: Changing user password.

### To change your password if it is expired:

On your computer, open Internet Explorer and type: <https://portal.dmh.mo.gov/>. Log into the portal. If your password is expired, you will see this page prompting you to change your password:

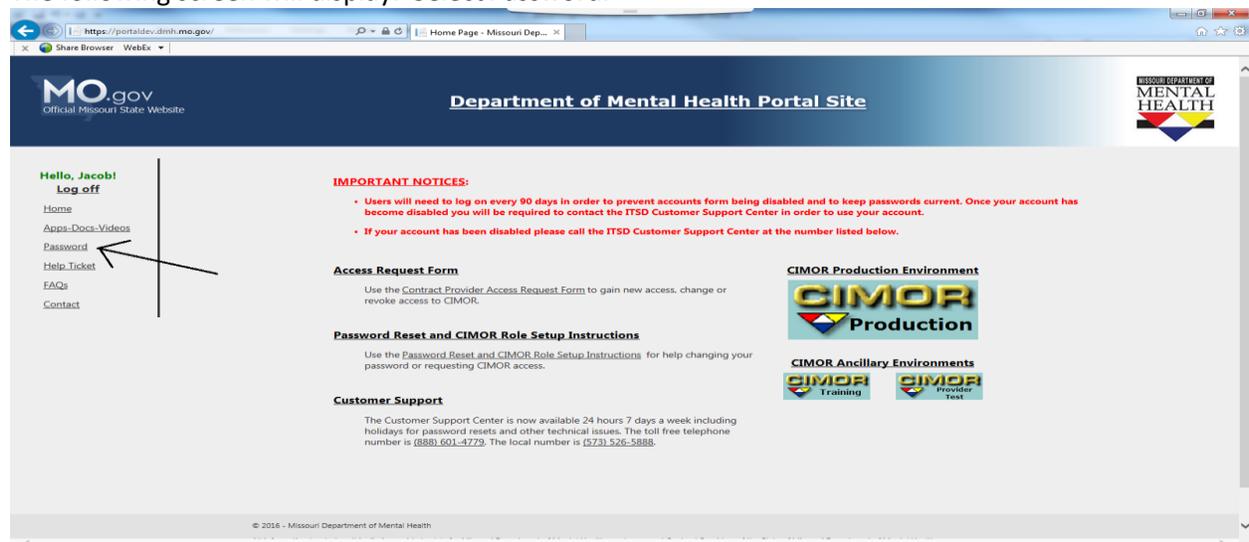


The screenshot shows the 'Department of Mental Health Portal Site' with a blue header. On the left, there is a navigation menu with 'Please log in!', 'Home', 'FAQs', and 'Contact'. The main content area displays the message 'Your password is expired, please change your password.' Below this message are links for 'Password Rules for EXTLCL Users' and a text prompt 'Domain\Username --> Example: "EXTLCL\myxxxxx"'. There are four input fields: 'Domain\Username', 'Password', 'New Password', and 'Confirm Password'. At the bottom, there are two buttons: 'Change Password' and 'Cancel'.

Fill in the Domain\Username, Password, New Password, and Confirm Password boxes. You will then click the Change Password box. If the password change was successful, it will take you back to the portal Login page. You have successfully changed the password and may now login with your new password.

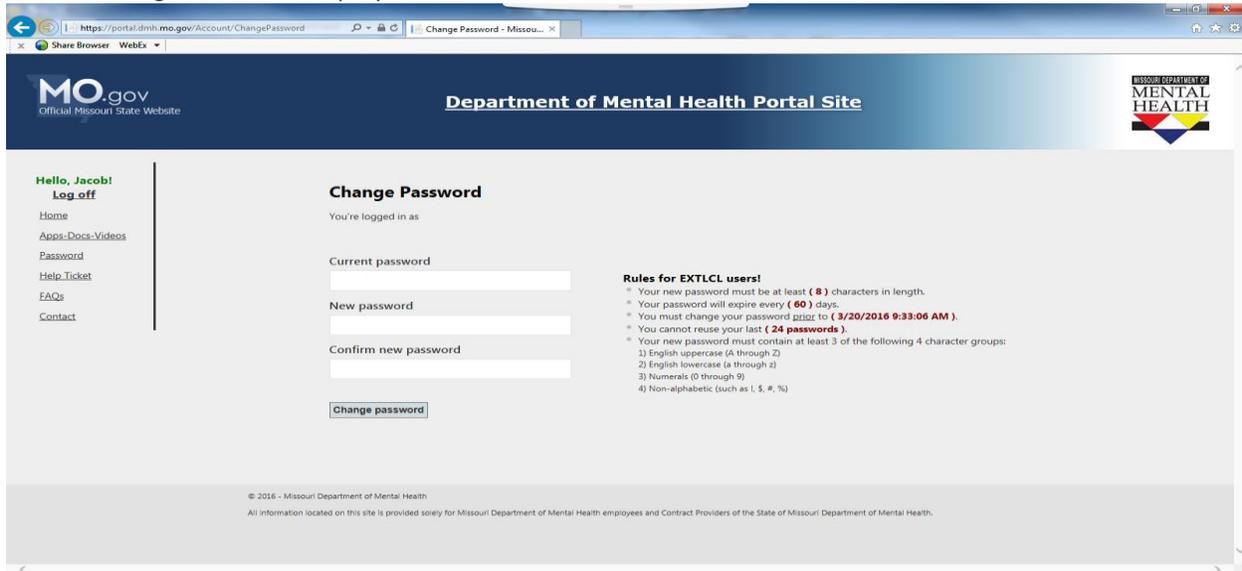
### To change your password before it expires:

On your computer, open Internet Explorer and type: <https://portal.dmh.mo.gov/>. Log into the portal. The following screen will display. Select Password.



The screenshot shows the user dashboard for 'Hello, Jacob!' with a 'Log off' button. The navigation menu includes 'Home', 'Apps-Docs-Videos', 'Password', 'Help Ticket', 'FAQs', and 'Contact'. A red arrow points to the 'Password' link. The main content area features 'IMPORTANT NOTICES' with two bullet points, 'Access Request Form', 'Password Reset and CIMOR Role Setup Instructions', and 'Customer Support'. On the right, there are logos for 'CIMOR Production Environment', 'CIMOR Ancillary Environments', 'CIMOR Training', and 'CIMOR Provider Test'. The footer contains the copyright information: '© 2016 - Missouri Department of Mental Health'.

The following screen will display:



Type in your current password, new password, confirm new password and select Change password.

“Your Password is successfully changed” will appear in the next screen.

## PART XI: Accessing Providers File Transfer Protocol (FTP)

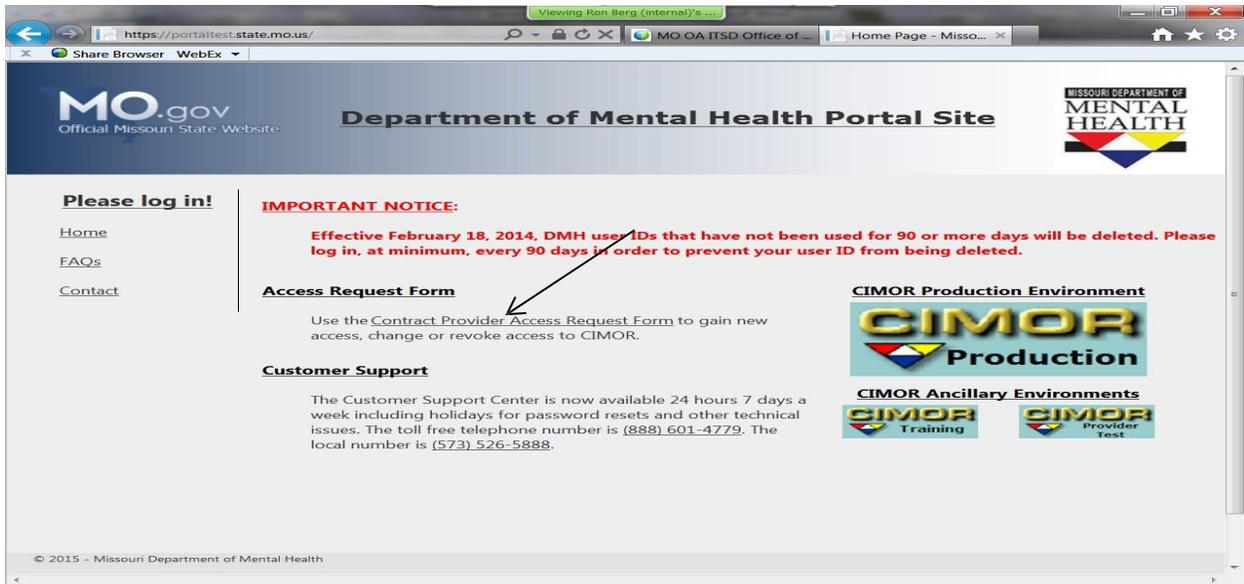
Every provider has an FTP available to them. The primary report in the FTP is CIMOR report which shows what the provider has input (for billing) into CIMOR and whether the data has been accepted or rejected. It is available the day after input. The FTP may contain additional information in the future as development permits.

The provider can request an employee’s access to the FTP when requesting initial access to CIMOR as described in Part II and Part III of this document.

To add this access to an employee who already has CIMOR access:

Complete the Contract Provider Access Request Form at <https://portal.dmh.mo.gov/>.

- Under Additional Data Request, all providers need at least one staff to indicate **FTP File**. If this employee will need access, enter this information. See Section XI for information about FTP to help you decide.



Fax completed document to your local Regional Office Provider Relations Liaison who will forward to OA.

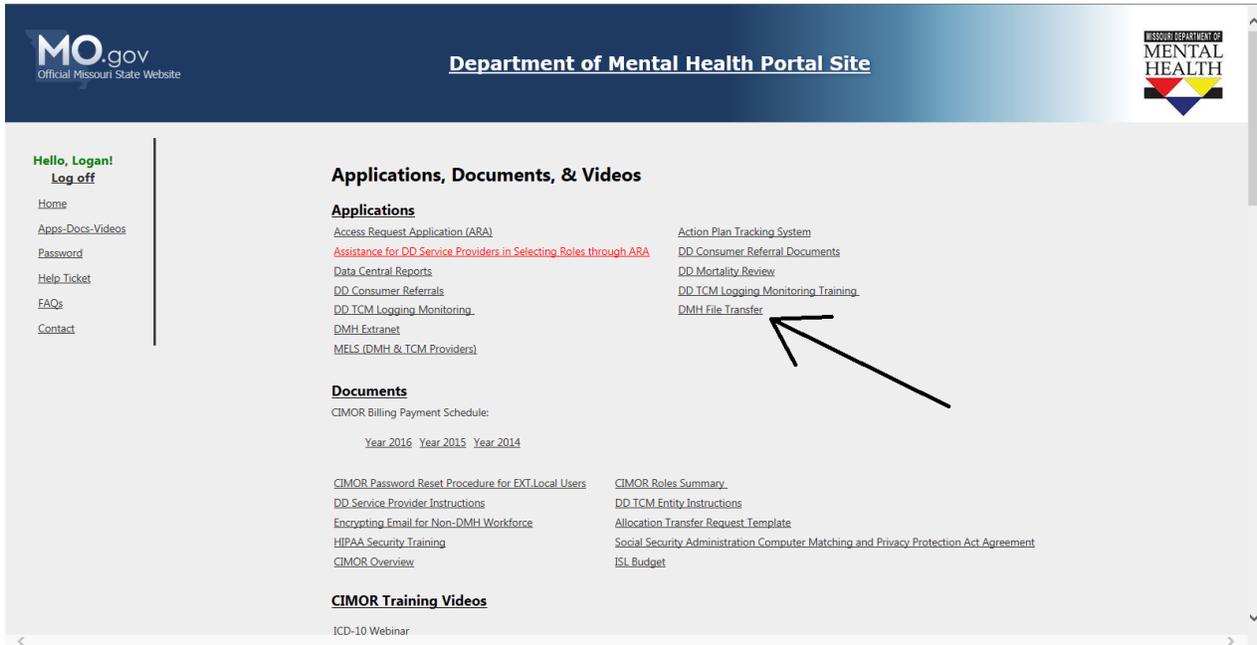
The employee will receive an email stating that their access to the FTP file has been granted.

Each FTE file is identified by the provider's unique facility code. The employee will need the facility code to open the correct file. To locate the facility code:

- Open your organization in CIMOR
- Click on "ID's" tab
- Under the Organization ID Type column locate Facility Code
- The code is indicated to the right under the column "Organization ID Value"

## Instructions for Accessing the DMH FTP Site for an Organization

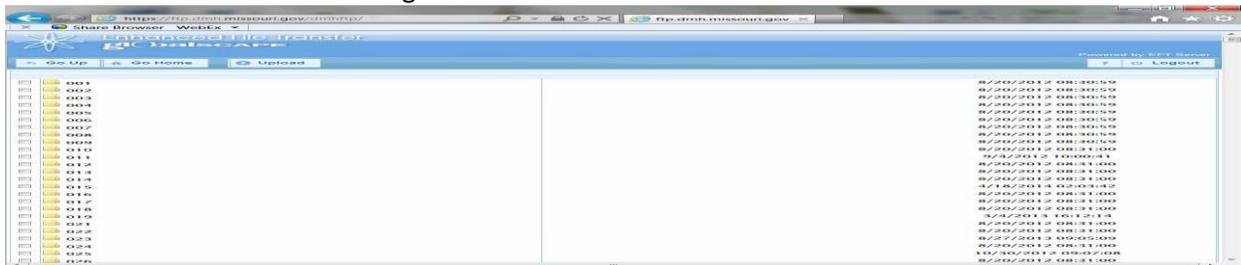
1. In Internet Explorer (or other web browser) go to <https://portal.dmh.mo.gov/> and log into the portal.
2. Click on App-Docs-Videos at the top of the page.
3. Choose the link labeled DMH File Transfer.



4. Enter your DMH-supplied username and password in the pop-up window after clicking the link above:



You will be routed to the following screen:



5. Double click on your facilities code. You should see a folder called Reports. Double click the icon, then double click the MRD folder. This will give you access to all the folders and files in the FTP site.