ADMINISTRATOR USER GUIDE

ALABAMA ONE HEALTH RECORD

Unify™ Data Management Platform 2012/2013
Software Build 5.15

April 2015

Proprietary and Confidential Property of Truven Health Analytics Inc.

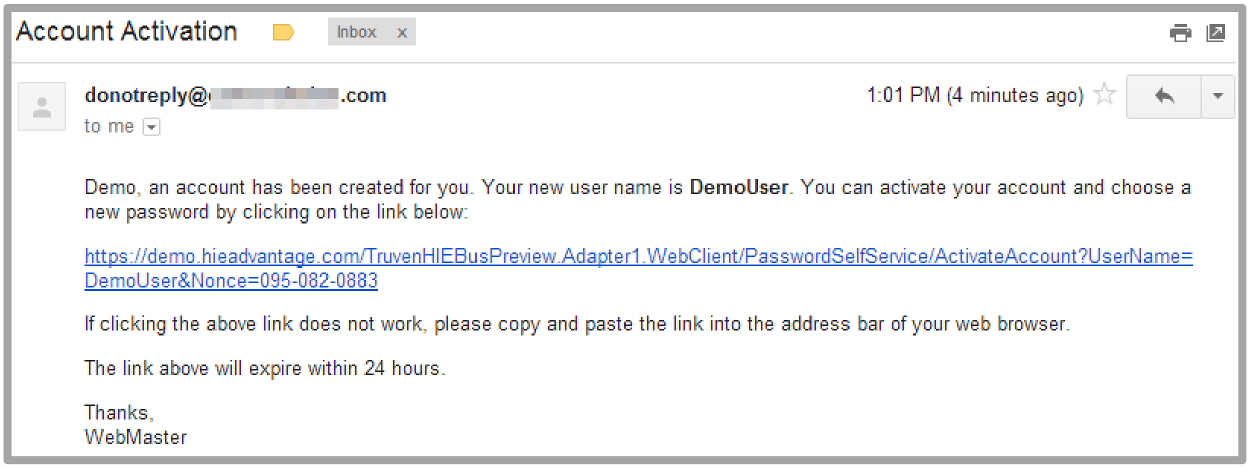
TABLE OF CONTENTS

INTRODUCTION

The purpose of this document is to provide a guide to essential information necessary for administering user access and security at your institution.

ACCOUNT ACTIVATION

New users will receive an email similar to the one below with a link to set up security questions and choose a password. Click on the link to begin account activation.



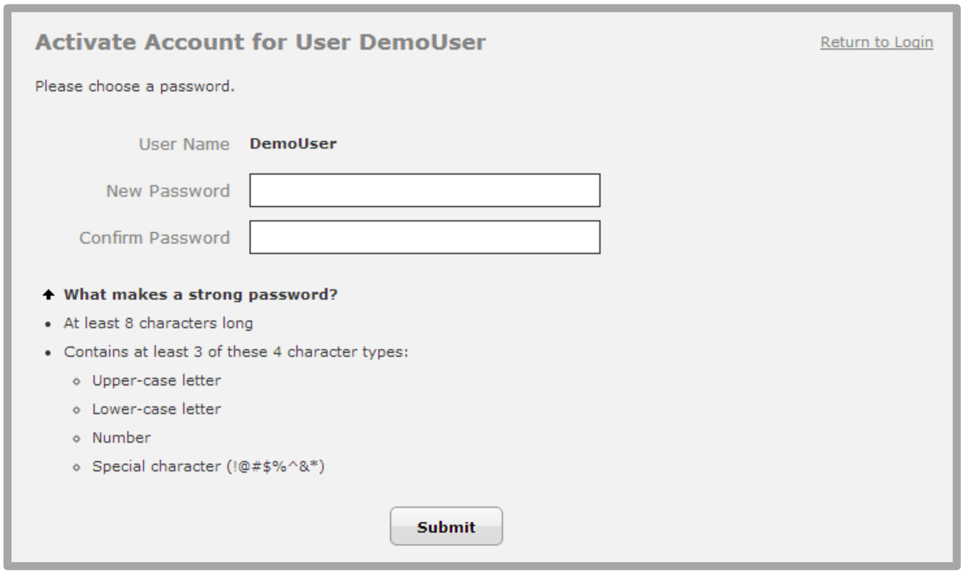
Note: The Clinical Web portal supports the latest versions of the following browsers:

- Google Chrome
- Internet Explorer
- Mozilla Firefox
- Safari

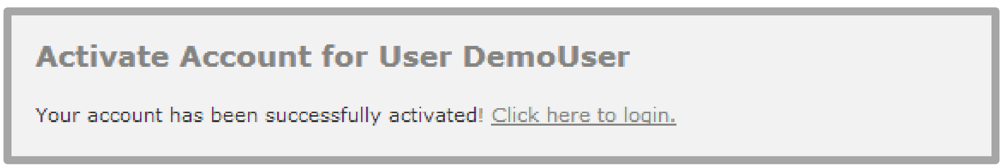
Once you click on the link to begin account activation, you will be directed to the following screen in your default Web browser.

Create a new password. To view the minimum requirements for your system, click the arrow beside **What makes a strong password?**. Enter your password and confirm, then click **Submit**.

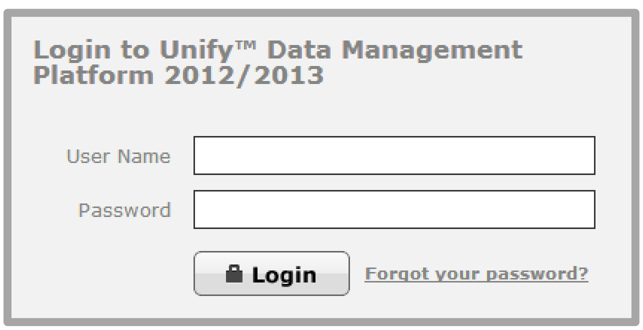
Note: Passwords are case-sensitive.



After your new password is accepted, you will see a confirmation screen. Make note of your user name before proceeding (the user name is “DemoUser” in the example below). Select **Click here to login**.



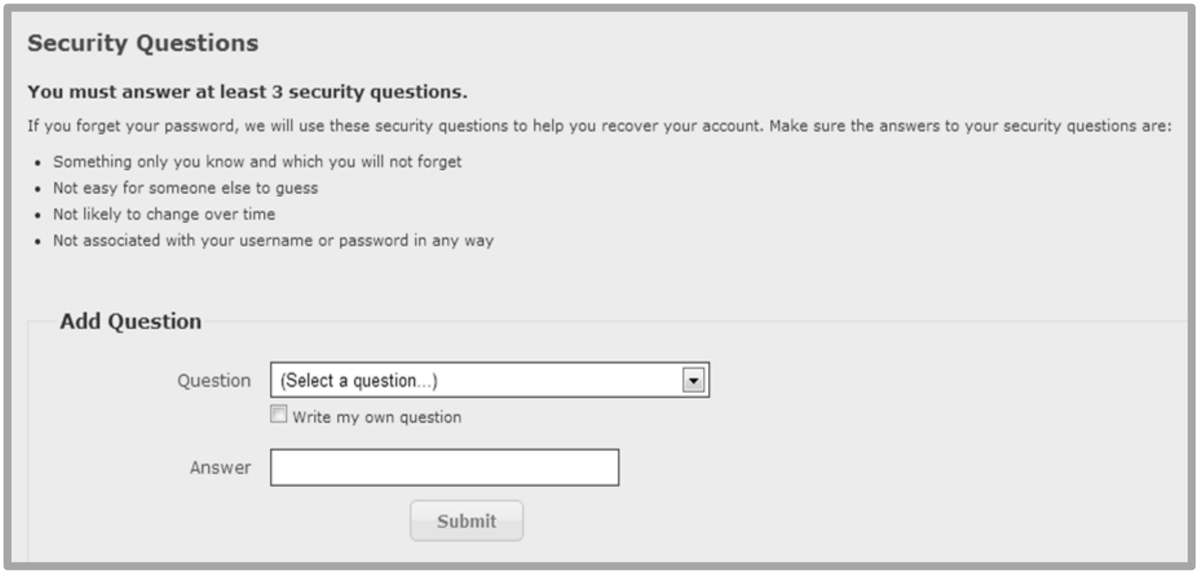
You will be taken to the login screen. Enter your username and password and click the **Login** button.



If you attempt login using the incorrect password too many times, your account will become locked out. Locked accounts will become unlocked after a certain amount of time. If you are having difficulties logging into your account, click the **Forgot your password?** link, or contact your system administrator.

Follow the directions to add at least three security questions. You may edit these later, after completion of the account activation steps, by clicking **My Profile** in the top right-hand corner of the screen.

Note: Prior to arriving on the *Security Questions* page, you may need to read and accept some terms and conditions, if they have been set by your HIE.

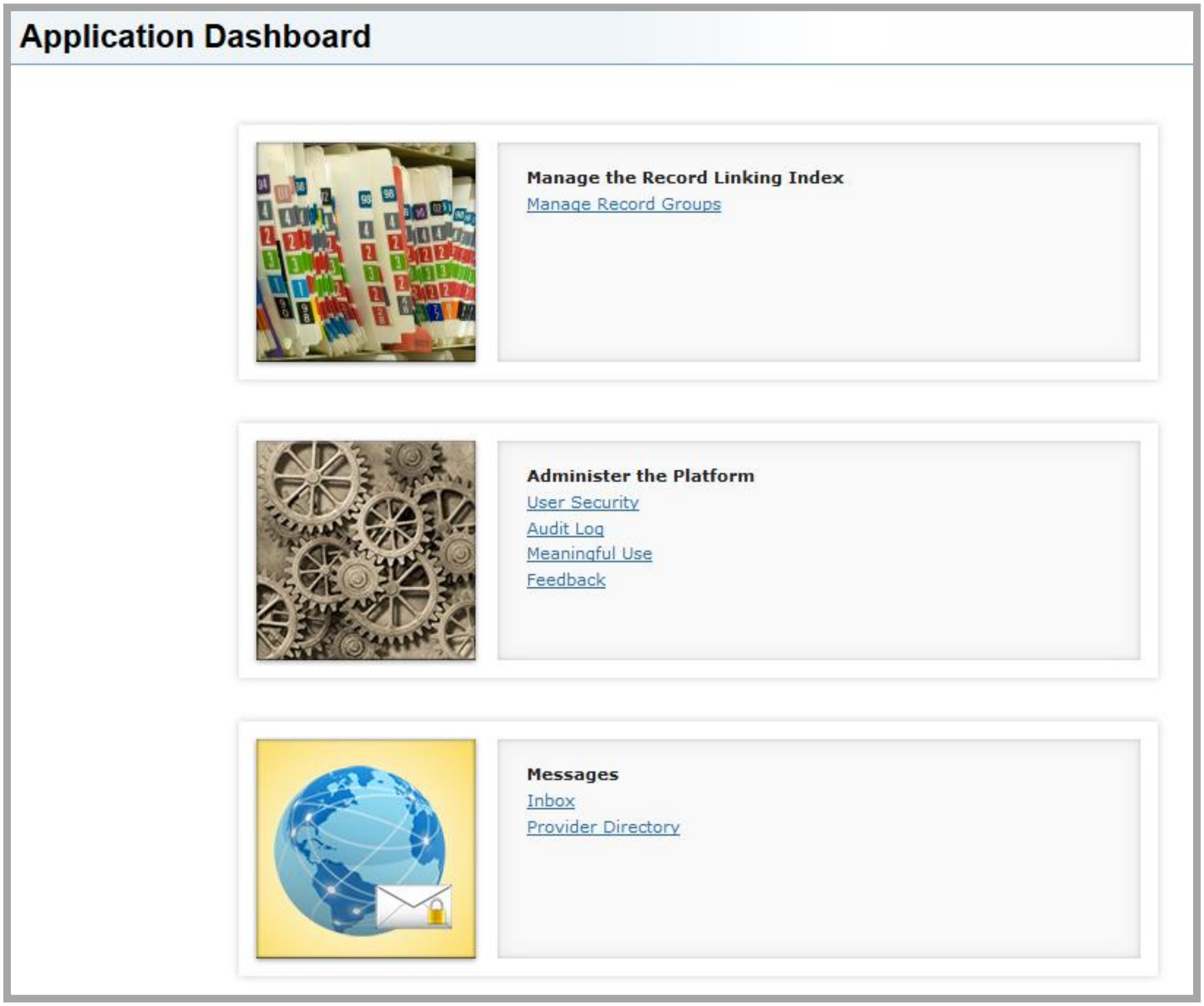


After adding your third security question, your account will be active and you will be redirected to the Application Dashboard “home” screen.

Note: Users with the Clerk role will be redirected to the *Census* screen.

APPLICATION DASHBOARD

After login, you will see the Application Dashboard, which functions as a “main menu” or “home page” of options. Depending on the permissions associated with your account, you may see different applications from those listed below.



NAVIGATING IN THE WEB CLIENT

The HIE platform's navigation bar allows for quick streamlined navigation through the various screens available within the Web client.

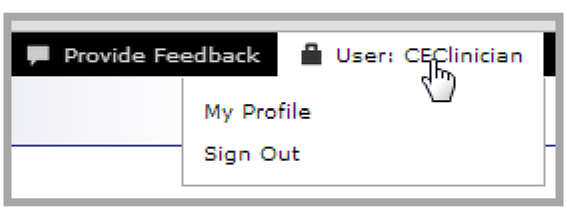
The menu links across the left-hand side correspond to the applications that are available to the user and reflect the permissions associated with the user's account. Depending on what those permissions are, different applications from those included in the screenshots below may appear on the navigation bar.

After a user has moved from the Application Dashboard "home" screen, a **Dashboard** button will appear, along with a "home" icon, at the left-most side of the navigation bar. This will provide access to the Application Dashboard from anywhere in the Web client. Note that the **Dashboard** button will not appear while a user is on the Application Dashboard.

After a user has accessed additional applications, a link to the most recently accessed application will appear next to the **Dashboard** button. This **Back** button is indicated by a back arrow with the name of that screen.

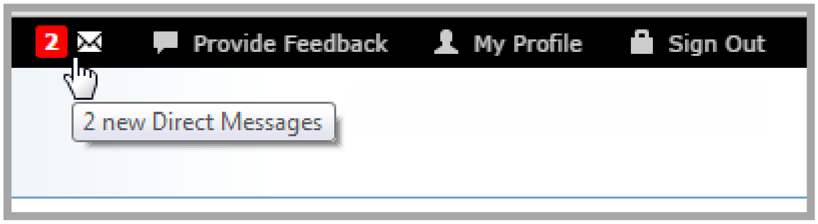
Hovering over any of the menu links, not including the **Dashboard** button or the **Back** button, will display a dropdown menu containing menu options, again corresponding with those listed on the Application Dashboard.

Across the right-hand side of the navigation bar are additional menu links. By hovering over the user name, the *My Profile* and *Sign Out* links become visible. Refer to the **Feedback** and **My Profile** sections below, if applicable, for additional information.

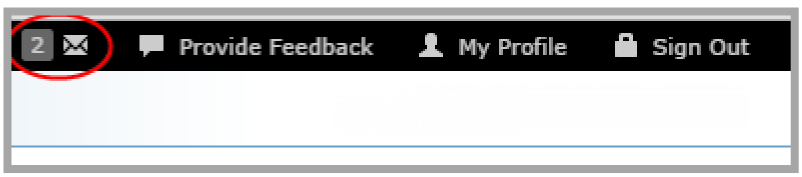


These links may also be configured to provide access to the My Profile and Sign Out buttons via individual buttons.

For users that have access to the Direct secure messaging application, a message notification may appear on the navigation bar. This notification displays the number of unread messages in a user's Inbox. When new messages are received, the indicator displays in red.

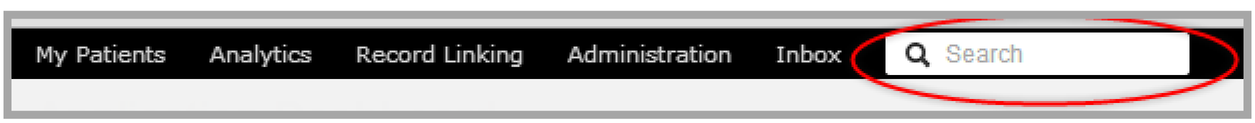


Clicking on the indicator will provide access to the Inbox screen. After the user has visited the Inbox, the indicator display will change from red gray.



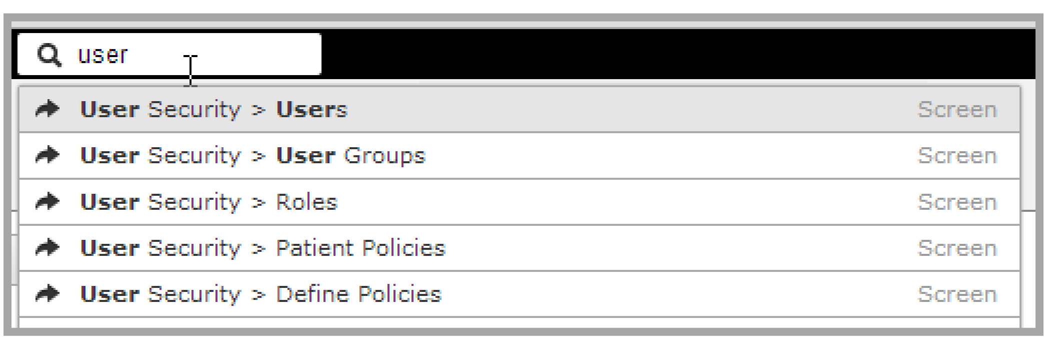
Global Search Bar

The Global Search Bar is located at the end of the menu links on the left-hand side of the navigation bar. It is useful for searching and navigating directly to a user's record or to any application screen within the HIE platform. The search terms are not case sensitive, and the search results will appear in a pop-up window directly below the search box.

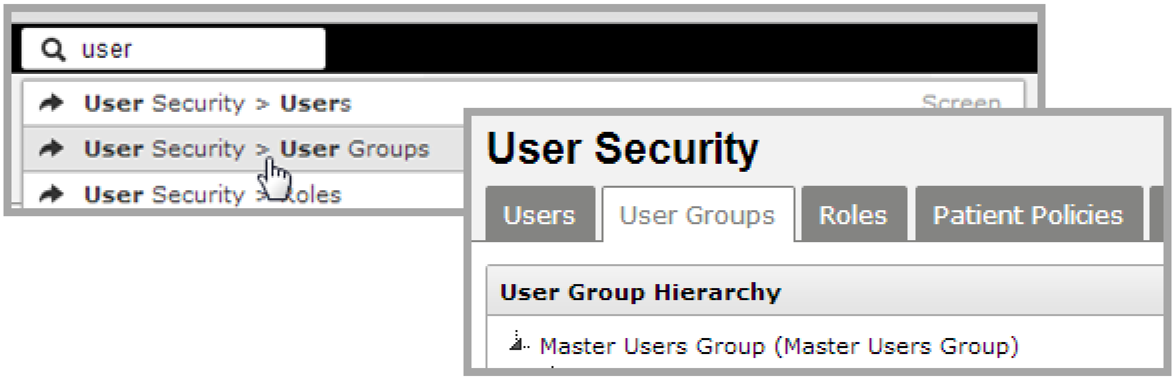


Searching for Screens

The search results will include all screens for which the search term is included as all or part of either the application name (e.g., User Security) or the tab names (e.g., Users).

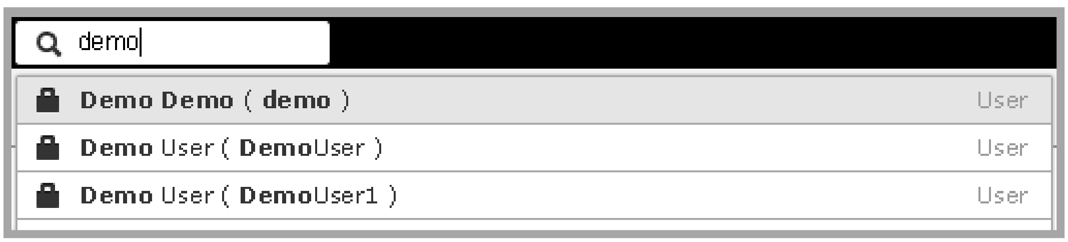


Clicking on a row from the list of results will provide access to that screen.



Searching for Users

The search results include all users for which the search term is the user's first name, last name, or username. Search results do not include any user records that only partly match the search terms.

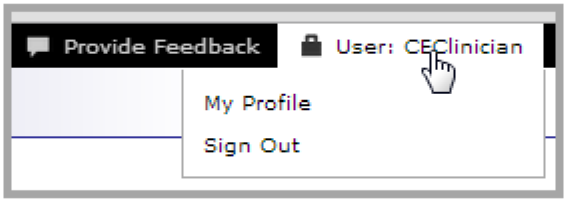


Clicking on a row from the list of results will provide access to the user's security record.

Because of this shortcut navigation feature, only users with the appropriate administrative permissions for accessing user security records will be able to use the global search bar to perform a search for users.

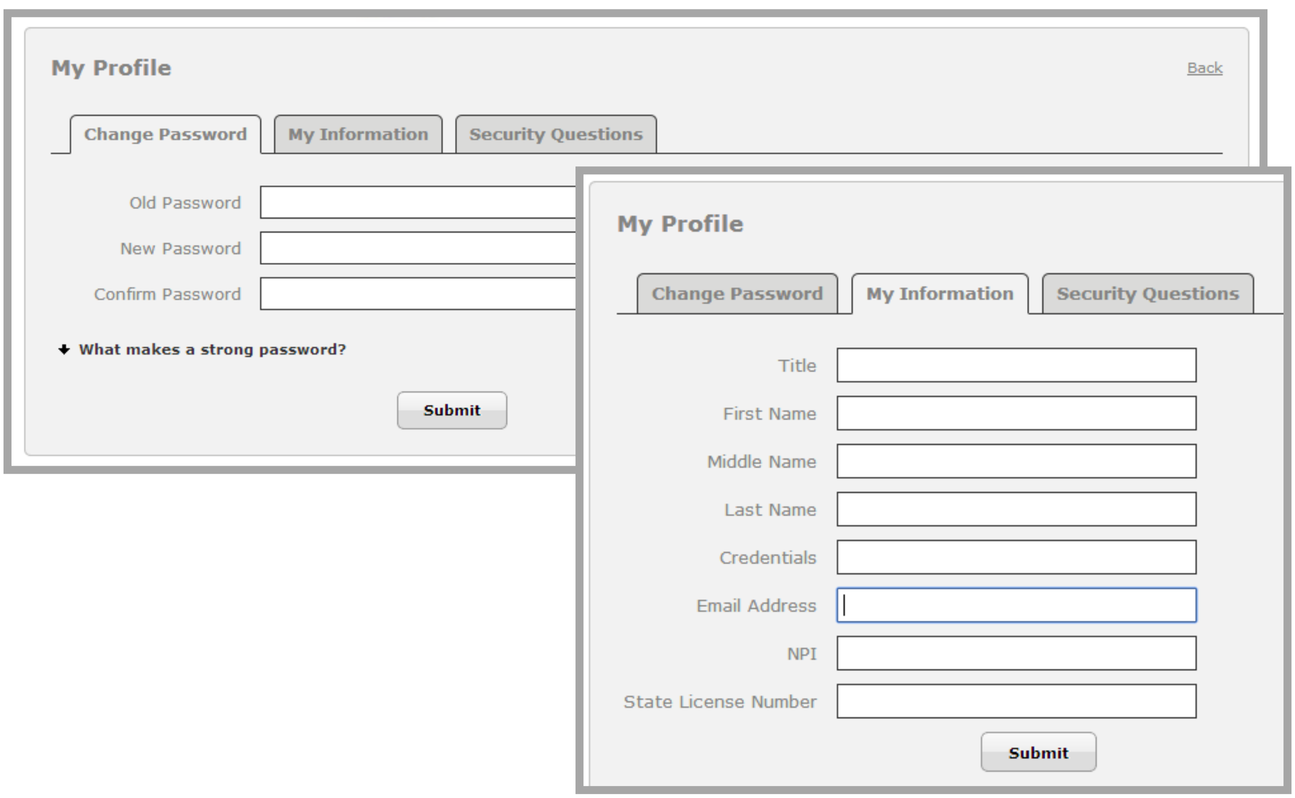
MY PROFILE

To change your password and update your security questions and answers, access your profile by hovering over your user name in the upper right-hand corner of the screen and selecting the **My Profile** link.

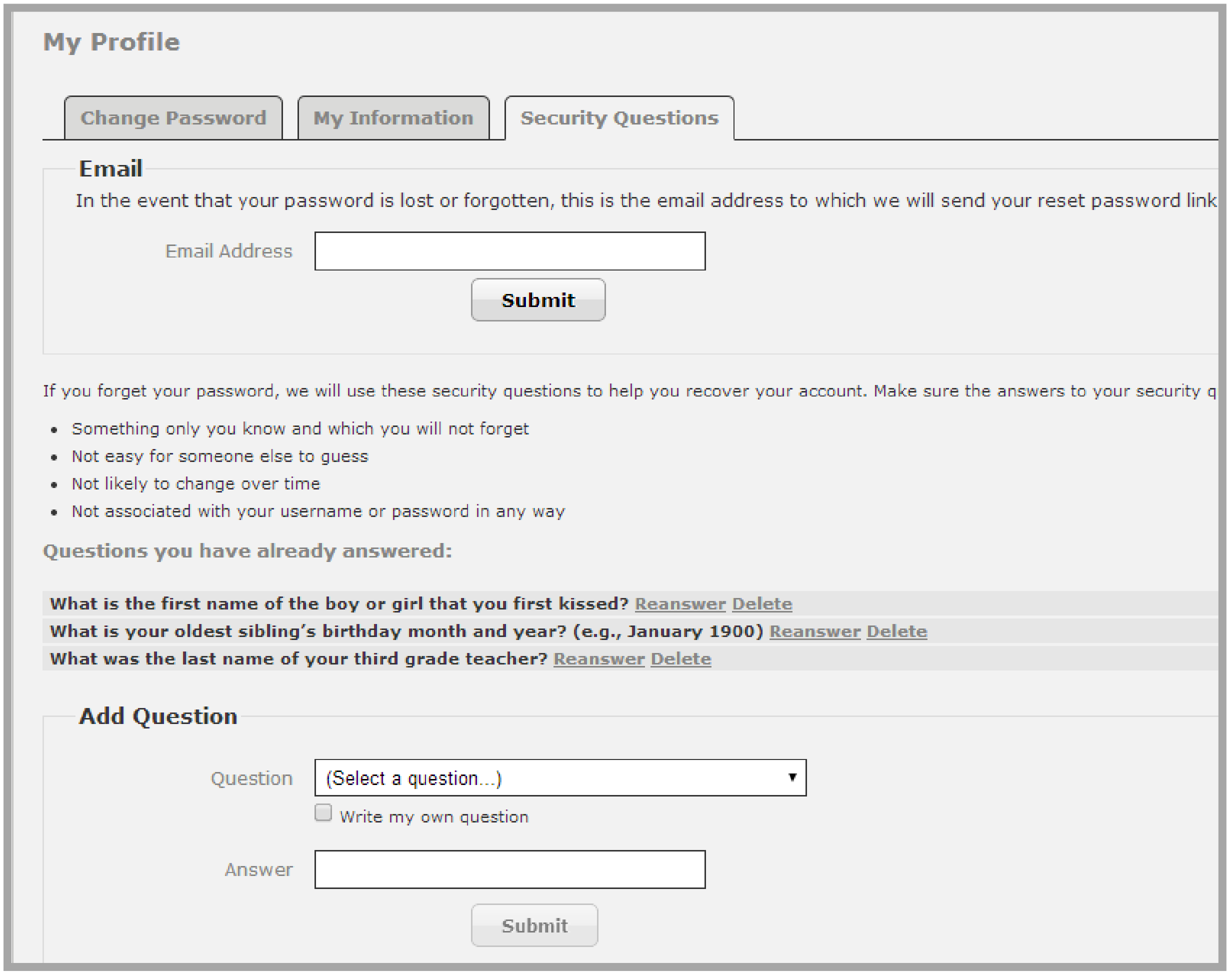


Note: The **My Profile** button may be available via a separate button on the navigation bar, instead of via a dropdown menu under the user name.

Here, you can update your password on the **Change Password** tab, view and update **My Information**, or update your **Security Questions**.



On the **Security Questions** tab, you can update the email address to which password reset links will be sent, and you can view and update your selected security questions.



Click the *Back* link on the right-hand side of the screen to return to the patient information tabs.

CREATING AND MANAGING USERS

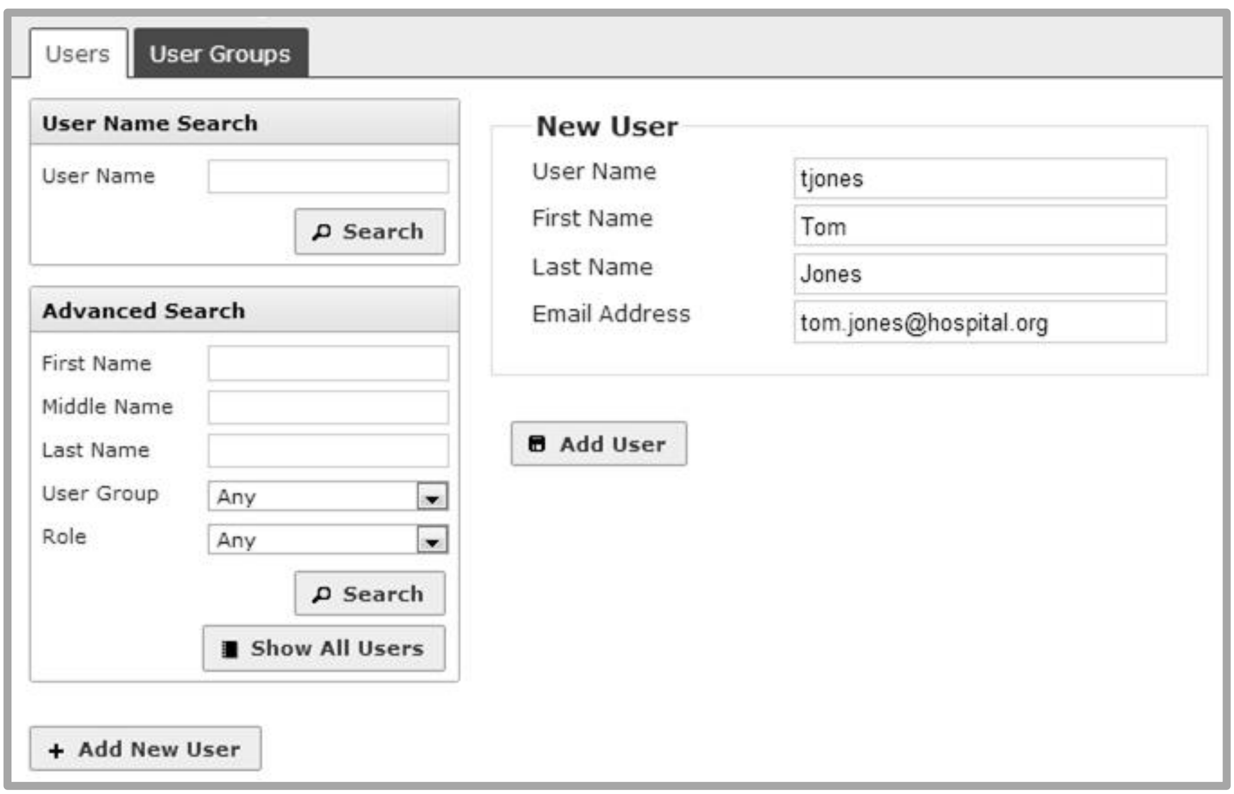
This section will detail how to add new users to the system, how to change system settings for existing users, and how to manage user password settings.

New User Profile

The steps to creating a new user are as follows:

1. Enter basic information (user name, first name, last name, and email address) to create the user account
2. Complete the “User Demographic” and “Contact Information” sections
3. Select “User Group Settings”
4. Assign “Roles”
5. Assign “Institutions”
6. Link account to external “Identifiers” (if applicable)

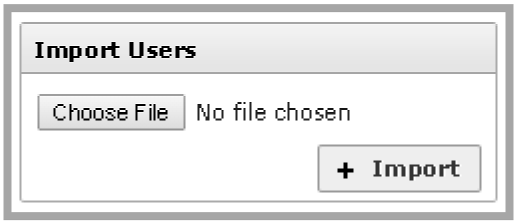
To begin creating and managing user accounts, click **User Security** from the Application Dashboard and select the **Add New User** button from the lower left-hand portion of the **Users** tab. Complete the text boxes that appear in the *New User* window on the right hand side, and then click **Add User** to create the new user account.



If a user name is already taken, you will get the following message: "The user name is already in use." If this occurs, select a different user name; consider adding a number to the end of the user name that was previously selected.

Importing Users

Large numbers of users can be added to the system using the *Import Users* function on the **Users** tab.



Information about users must be compiled in a comma-delimited text file (saved as a .csv file). The file must be set up as follows:

- Field 1: User name (required)
- Field 2: First name
- Field 3: Last name
- Field 4: Credentials
- Field 5: Email address (required)
- Field 6: Institution code

  Note: Multiple institutions can be listed by separating them with a pipe character.
- Field 7: User group code (required)
- Field 8: Role(s) (required)

  Note: Multiple roles can be listed by separating them with a pipe character.

Any Institution, User Group, or Role being assigned must already exist in the system.

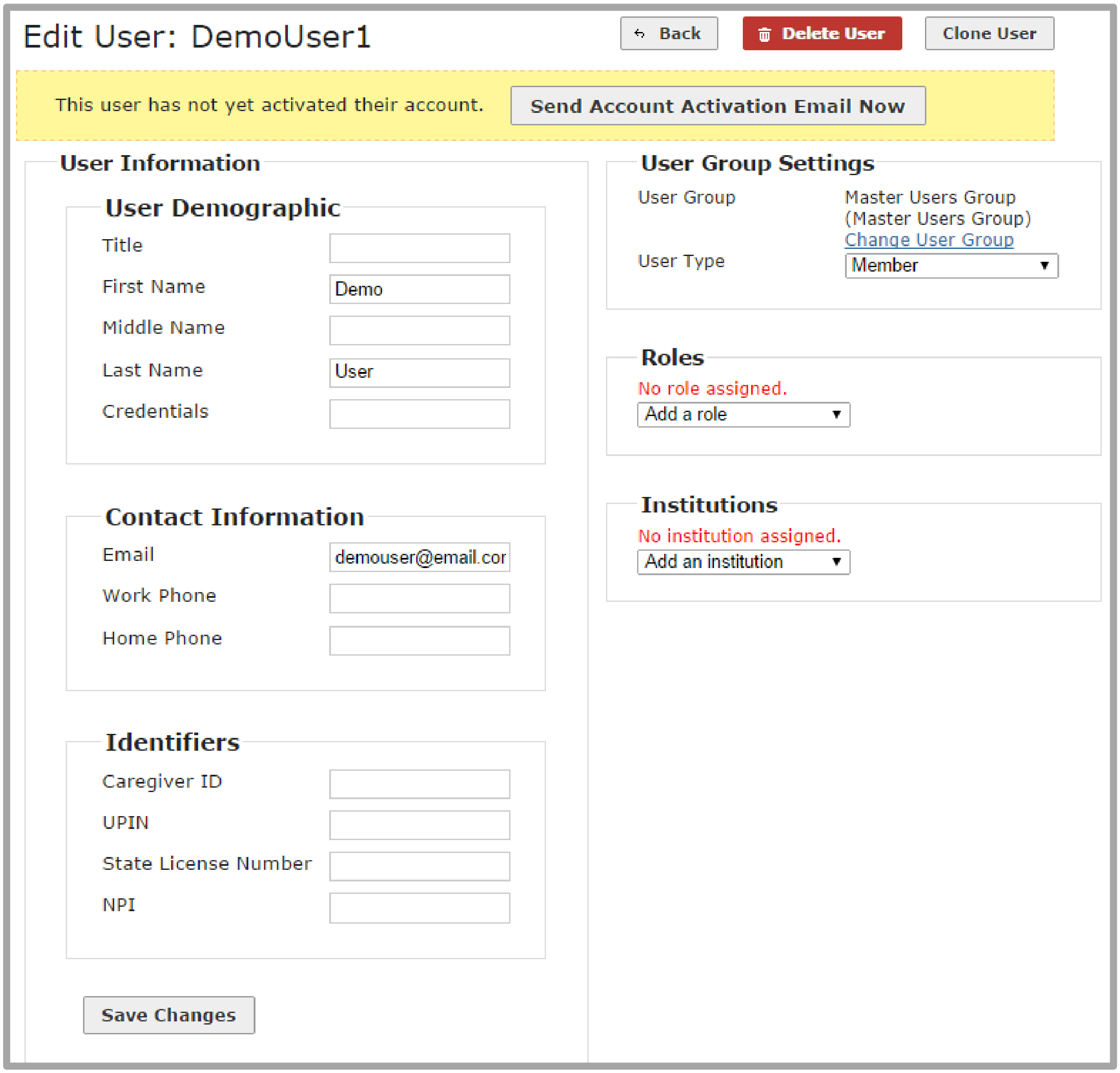
Note: The Institutions and User Group values currently expected are codes, not names. For more information about codes, contact the deployment team.

Here are two examples of user profiles for Joe Smith, MD, and Fred Jones using the correct CSV format:

```
jsmith,Joe,Smith,MD,joe_smith@email.com,HospitalA,Physicians,Clinician
fjones,Fred,Jones,,fred@email.com,HospitalA|HospitalB,Master User Group,Admin|PowerUser
```

Editing New Users

After adding a new user, you will immediately be taken to the **Edit User** screen below. You will need to enter **User Demographics, Contact Information, Identifiers, User Group Settings**, and assign **Roles** and **Institutions**. You should complete as much of the information on this page as possible before activating the account. Specifically, the *First Name*, *Last Name*, and *Email* fields must be completed in order to create a new user. Once all available information has been entered, click the **Save Changes** button.



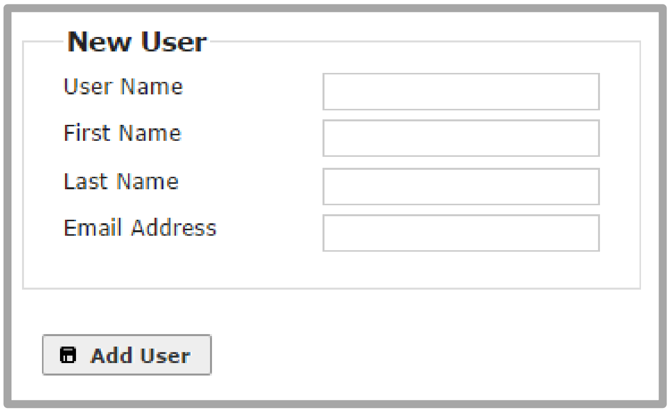
The **Send Account Activation Email Now** button at the top of the user account page allows the Administrator the option of immediately sending the account activation link or waiting until later (e.g., when creating multiple user accounts for a group go-live event).

If the account was created in error, click **Delete User** at any time during the process. The user name will be made immediately available for use again in the system.

Cloning Users

If the selection of user groups, roles, and institutions will be the same for multiple users, the **Clone User** button can be used to copy that part of a user's configuration to another new user.

After making selections in the *User Group Settings*, *Roles*, and *Institutions* sections, click on the **Clone User** button. The *New User* screen will appear. Enter the new user's user name, first name, last name, and email address, and then click the **Add User** button.



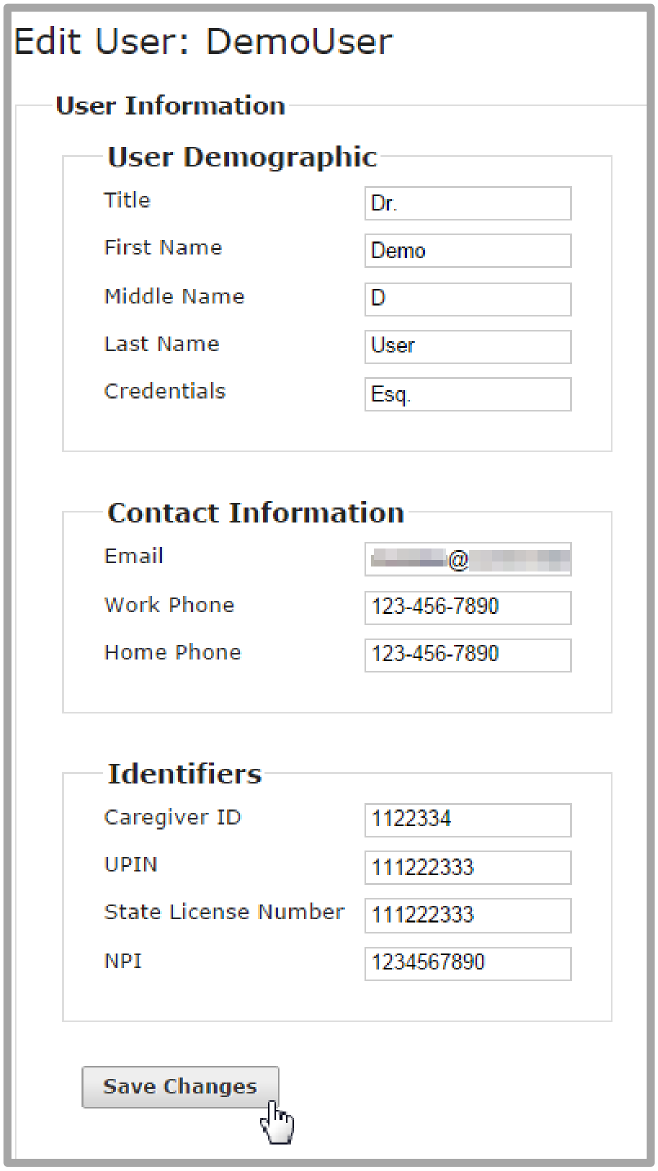
All of the user groups, roles, and institutions will be copied to the new user. However, note that none of the demographic information will be copied.

User Information

The *User Information* section of the *Edit User* screen contains all of the user's demographic information. All available user information should be entered, including the user's title, middle name, and credentials, if available. Examples of credentials include MD, DO, and RN.

Contact information is extremely important for support purposes. Email and work phone should always be included, in the event that a support ticket is opened or the user needs to be contacted.

The National Provider Index (NPI) should be included for all providers, as this enhances the functionality of the Provider Directory (if applicable). If the user account represents a medical organization, utilize the appropriate Organizational NPI.

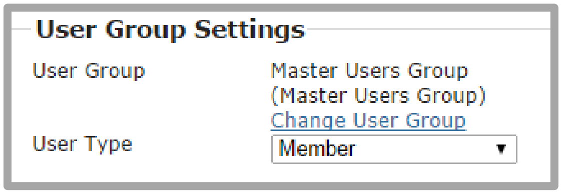


After entering any information, you must click **Save Changes**; otherwise, new information will not be recorded.

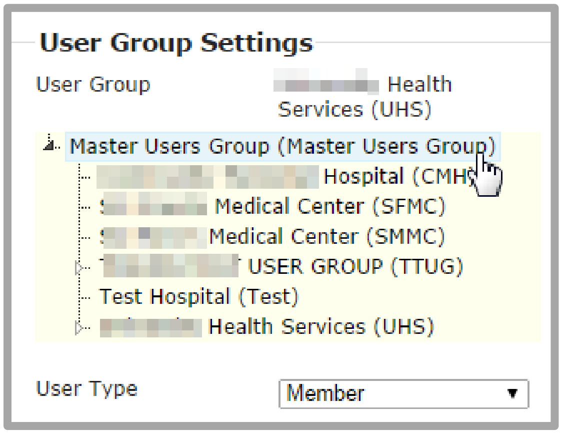
User Group Settings

By default, all users belong to the same user group as the person who created their account. User Group Administrators and all other users may be reassigned to a child user group, depending on affiliation. User Group Administrators can only add users to a group for which they have administrative rights or to a child of that group.

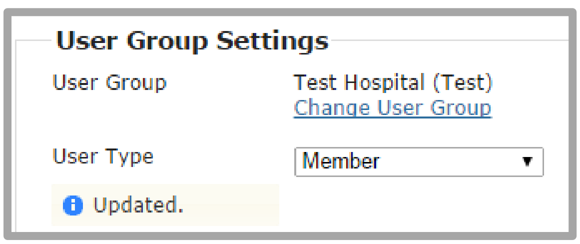
For more information on user groups, please refer to the **Managing User Groups** section.



To add the user to a child user group beneath a parent user group, click **Change User Group**. Select the appropriate user group from the list displayed.

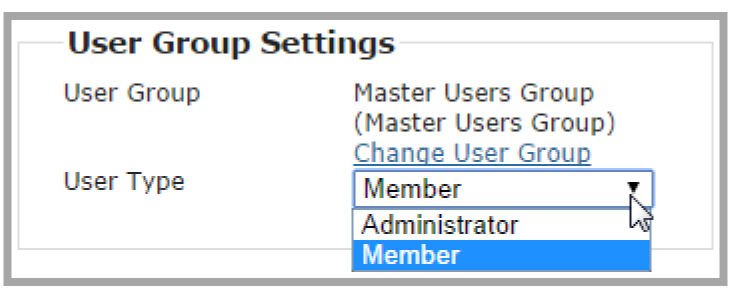


Once selected, the list will collapse, and a confirmation message will appear, indicating that the user group selection has been *Updated*.



Note: If the correct user group does not yet exist, see the **Managing User Groups** section for information on adding a new child user group.

Users must also be assigned a *User Type*. All non-administrators have a User Type of **Member** by default. For users who will be administering user accounts**,** select **Administrator**.



User Groups for Patient Portal Management

Users who will be managing user accounts for the Patient Portal must be assigned the PHR Account Creator role. Prior to provisioning users with this role, a separate child user group must be created, and all users provisioned with the PHR Account Creator role must be assigned to this user group. This will ensure that PHR Account Creators have only the access necessary to manage patient user accounts.

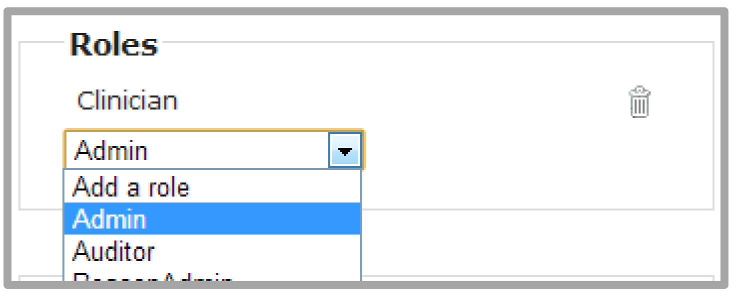
For more information on adding a child user group, please refer to the “Adding a User Group” section.

Roles

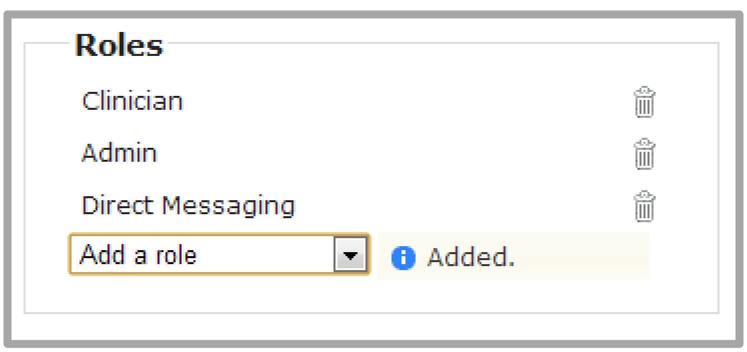
Roles ensure greater security and provide users with the appropriate functionality required for their responsibilities. Access granted to each role is based on system configurations as determined by Alabama One Health Record® policies.

A single user may be granted multiple roles, depending on their job requirements. For example, users with the Clinician role might only be able to view patient-related screens, while users with the Clerk role might only be able to view patient registration information.

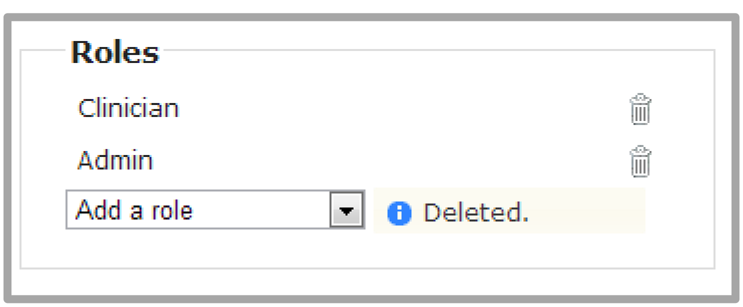
To add a role to a user account, select an option from the **Add a role** dropdown box.



To add more than one role, wait until the *Added* confirmation message appears, then select the next role, if applicable.



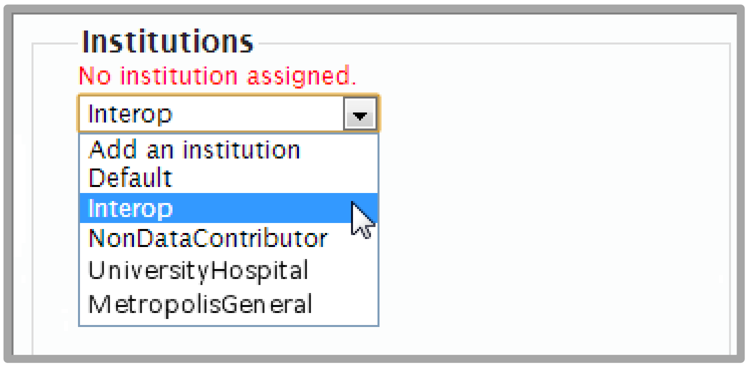
To delete a role, click on the trash can icon next to an added role. A *Deleted* confirmation message will appear briefly.



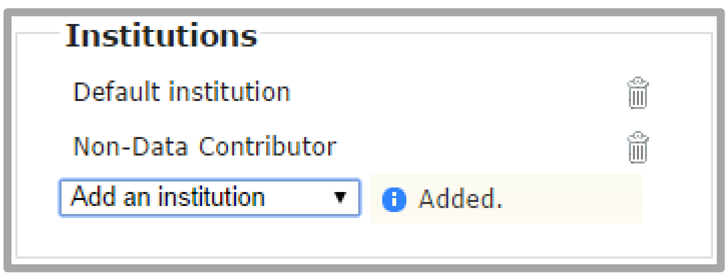
Institutions

Institutions represent the participating data contributors within the HIE. An institution might be a hospital, a practice, a state entity (e.g., Medicaid), an insurance provider, or another HIE. Each user must be associated with an institution in order to view patient data. Users may be associated with more than one institution.

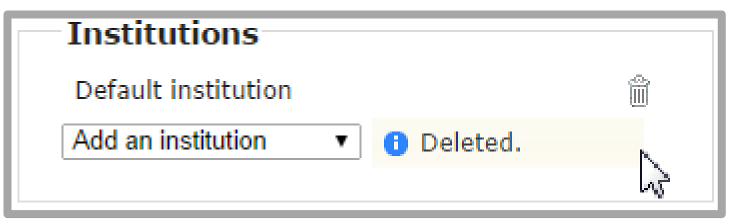
To add an institution to a user's account, select from the **Add an institution** dropdown. The institution will automatically be added to the user's profile.



Wait until the *Added* confirmation message appears, and then repeat the process to add additional institutions.



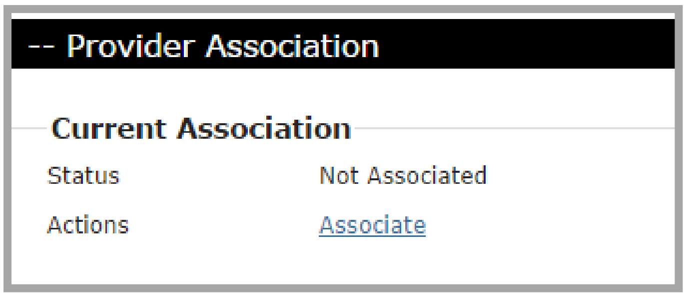
To delete an institution, click on the trash can icon next to an added institution. A *Deleted* confirmation message will appear briefly.



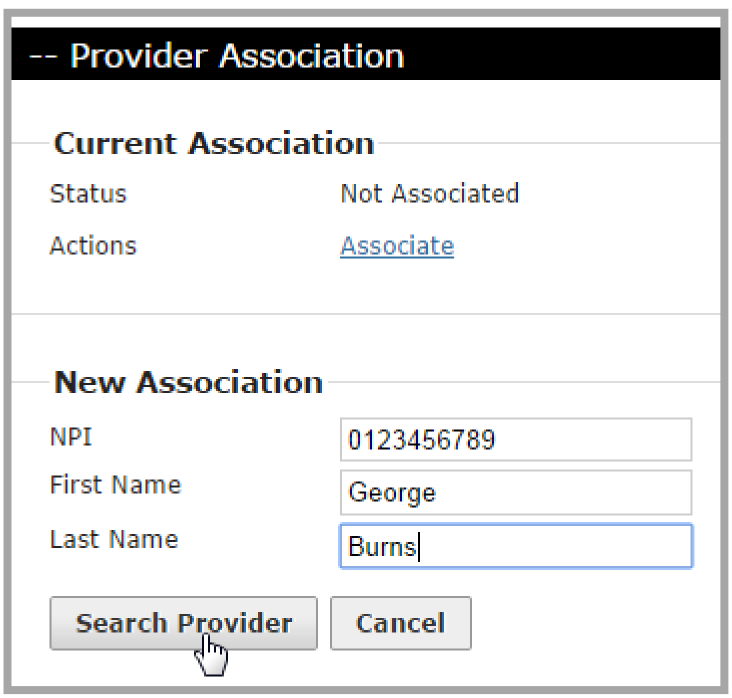
User-Provider Association

The Provider Directory contains information about care providers and other entities from the NPI Registry. The Provider Association feature on the *User Security* screen allows this information to be associated with a user account. In addition, it allows the Direct Messaging address to appear in the Provider Directory.

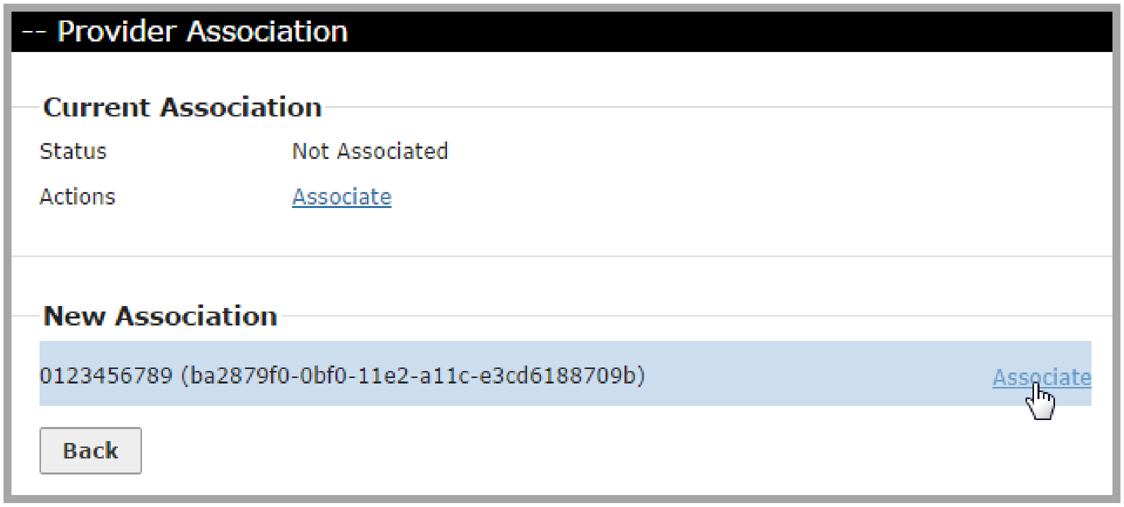
While viewing a user's account information on the *User Security* screen, click the **Provider Association** bar to expand the provider association window. Click on **Associate** to search for the provider.



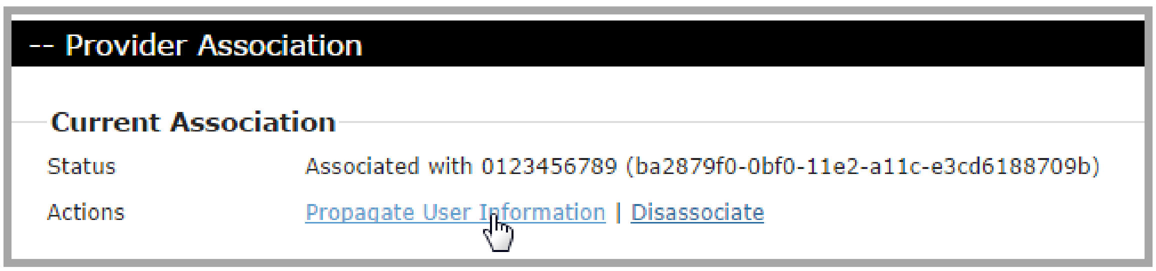
First Name and *Last Name* will be auto-populated from the basic user account information entered previously. Enter the provider's NPI, if known, to narrow the search.



Once you click the **Search Provider** button, results of the search will appear under *New Association*. Click **Associate** beside the correct result.



The user account is now associated with the entry in the Provider Directory. Click **Propagate User Information** to auto-populate data from the NPI Registry with corresponding fields in the user account.



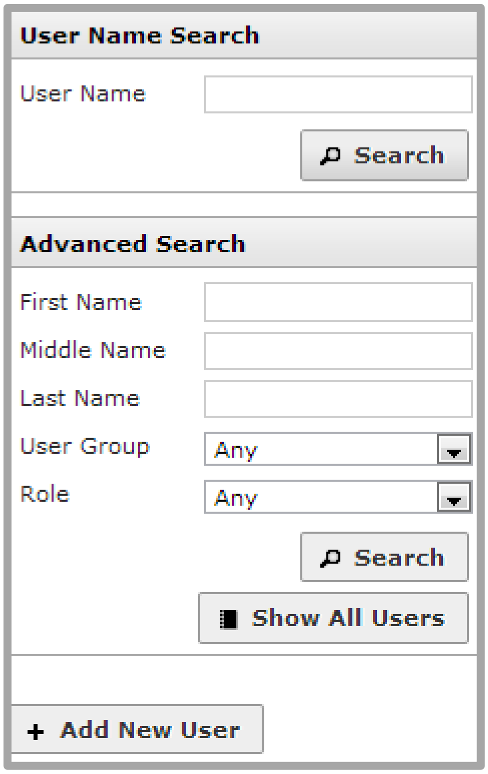
If the association was made in error or later needs to be removed, click **Disassociate** to remove the association.

Note: Any unwanted information that was previously imported from the NPI Registry must be manually removed.

Editing Existing Users

The tools at the left of the screen allow a search for user accounts to be performed. To locate a single account, use the “User Name” search; the exact user name must be entered to return a result.

Using the “Advanced Search” returns all accounts that match the search criteria. Search results will appear to the right of the search tools.



Searches that match exactly, or a successful user name search, will take you directly to the *Edit User* screen. Searches with more than one possible match will display a list of users. Click anywhere on the row containing the desired username to be taken to the *Edit User* screen.

Users

Full Name	Roles
Clinician Test	Clinician
Delegation Test	Clerk,Clinician
Direct Test	Direct Messaging Admin
Rhonda Test	Admin
User Test	
User Test	Clinician,Direct Messaging,BeaconAdmin
Will Test	Patient
Will Test	BeaconSurveillance

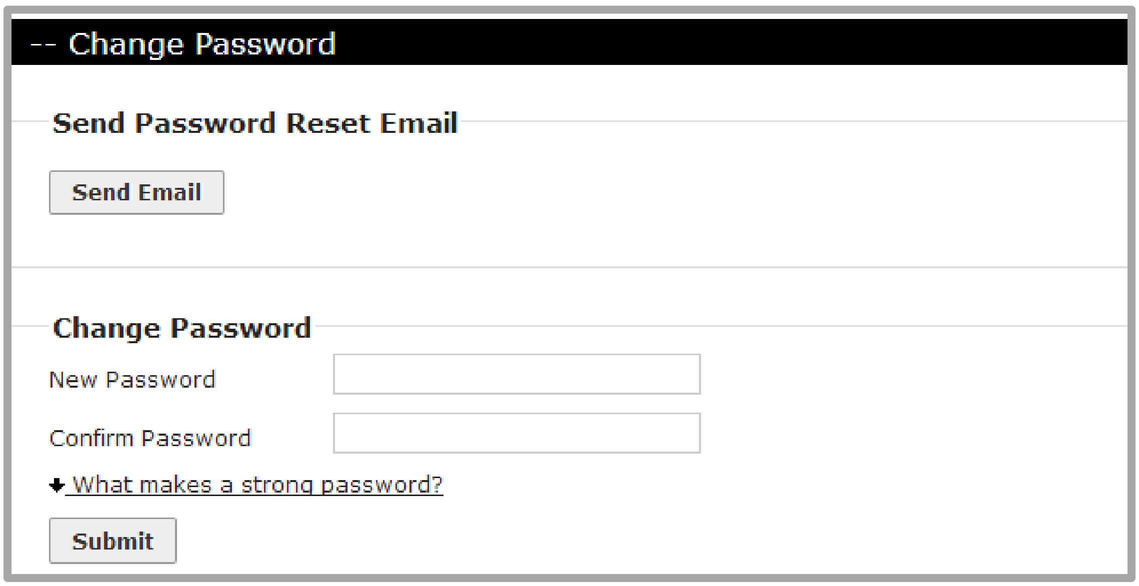
Showing 1 to 8 of 8 entries

Password Management

To change a user's password, scroll down below the user information to **Change Password** and click anywhere on the section header to expand it.

Two options will appear: **Send Password Reset Email** and **Change Password**.

- **Send Password Reset Email:** Clicking the **Send Email** button will send a password reset email to the user's listed email address. This option will only appear if the user account contains an email address. It can only be used if the user has set security questions.
- **Change Password:** A user's password can be changed by entering and confirming a new password for the user.



Passwords must be at least eight (8) characters long. For greater security, Alabama One Health Record® policies dictate that passwords should conform to the guidelines that appear when the **What makes a strong password?** link is clicked. Strong passwords are defined as being:

- At least 8 characters long
- Contains at least 3 of these 4 character types:
  - Upper-case letter
  - Lower-case letter
  - Number
  - Special character (!@#$%^&*)

Password Expiration

Passwords expire every 90 days, as set by Alabama One Health Record® policy.

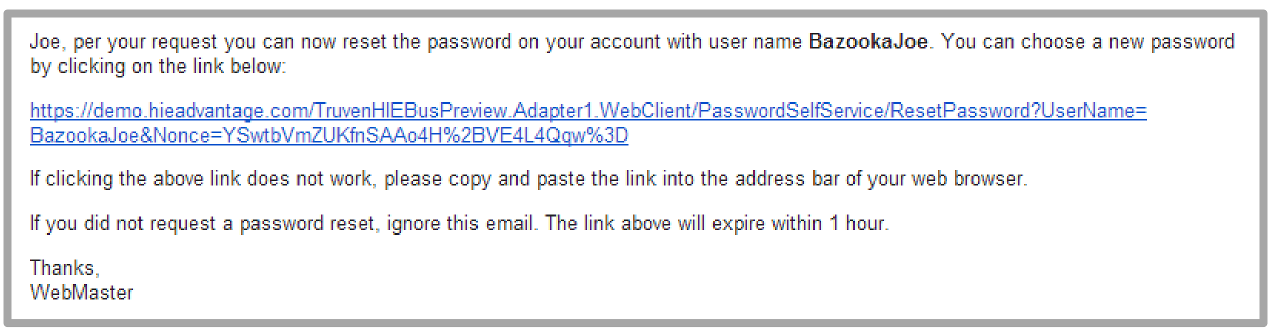
A user whose password is about to expire will see a warning window when they log in. Users may choose either to change their password at that time or to wait until a later time. Expired passwords must be changed in order to regain access to the system.

Note: By default, this warning will not be shown to any user with the Administrator role. The warning can be enabled by a system administrator.

Password Self-Reset

Users who have forgotten their password may perform a self-reset using the **Forgot your password?** link on the login page. After clicking this link, the user will be taken to the screen below.

After submitting a valid user name, a reset email will be sent to the user.


Joe, per your request you can now reset the password on your account with user name **BazookaJoe**. You can choose a new password by clicking on the link below:

https://demo.hieadvantage.com/TruvenHIEBusPreview.Adapter1.WebClient/PasswordSelfService/ResetPassword?UserName=BazookaJoe&Nonce=YSwtbVmZUKfnSAAo4H%2BVE4L4Qqw%3D

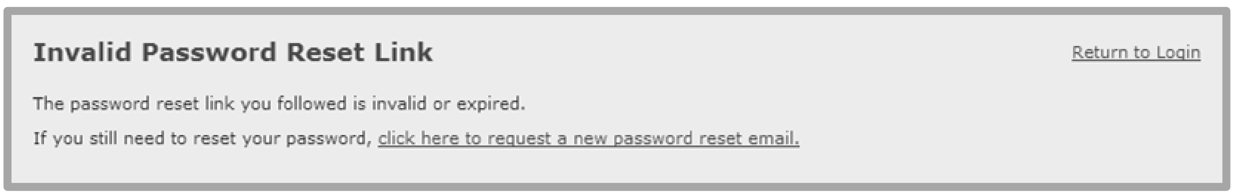
If clicking the above link does not work, please copy and paste the link into the address bar of your web browser.

If you did not request a password reset, ignore this email. The link above will expire within 1 hour.

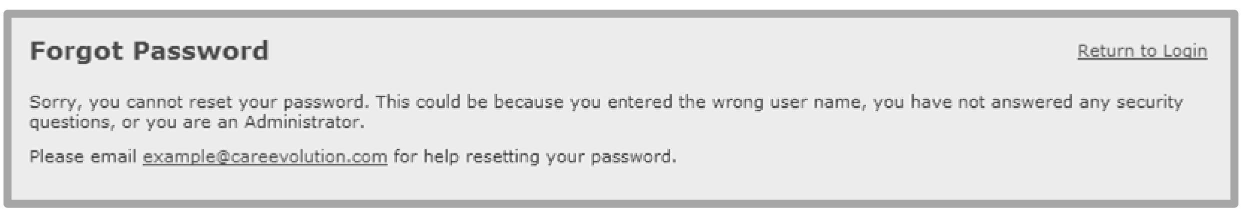
Thanks,
WebMaster

Clicking the link within the email will take the user to a screen to answer a security question and create a new password.

If the 48 hour time limit has expired (configured in compliance with Alabama One Health Record® policy), the user will see the following screen and may restart the process by clicking the link.



If the user has forgotten their username, has not answered security questions, or is an administrator, they will receive the following message. For security purposes, administrators must have another administrator manually reset their password using one of the options found in the “Password Management” section.



Note: Although administrator accounts can be given the ability to perform a self-reset in system configuration settings, it is not recommended due to security considerations.

Automatic Account Lock-out

If a user attempts to login to an account and repeatedly fails to provide the correct password, the account for that username will be locked for a certain period of time. This lock-out period helps to prevent unauthorized users from accessing the system by repeatedly guessing passwords.

The number of failed login attempts allowed before an account lock-out is triggered (5 attempts) and the duration of the lock-out (15 minutes) are both determined by Alabama One Health Record® policy.

MANAGING USER GROUPS

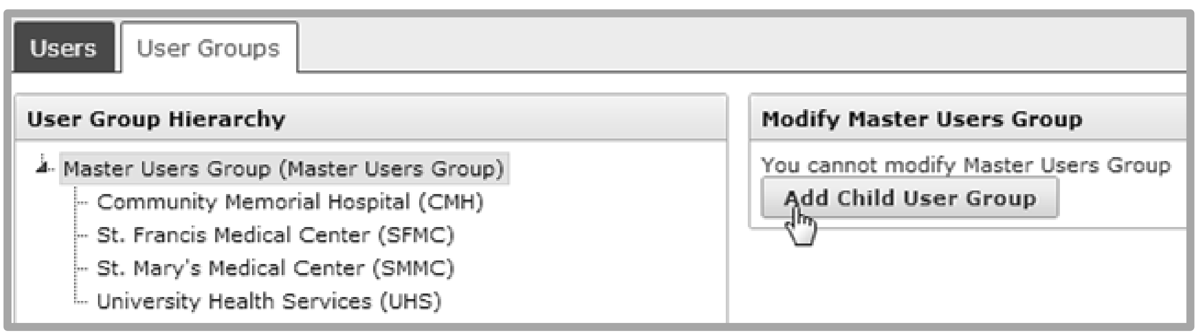
To better manage the HIE system, administrative users should become familiar with the operation of user groups.

User groups allow account settings to be applied to multiple users at one time. User groups are also used to assign user management capability to an administrative user for only a subset of the full user population. The most common application of this concept is to a site level administrator who will be responsible for creating and maintaining users at a hospital or clinic. Direct Messaging Administrators are only able to view user groups; they cannot manage them.

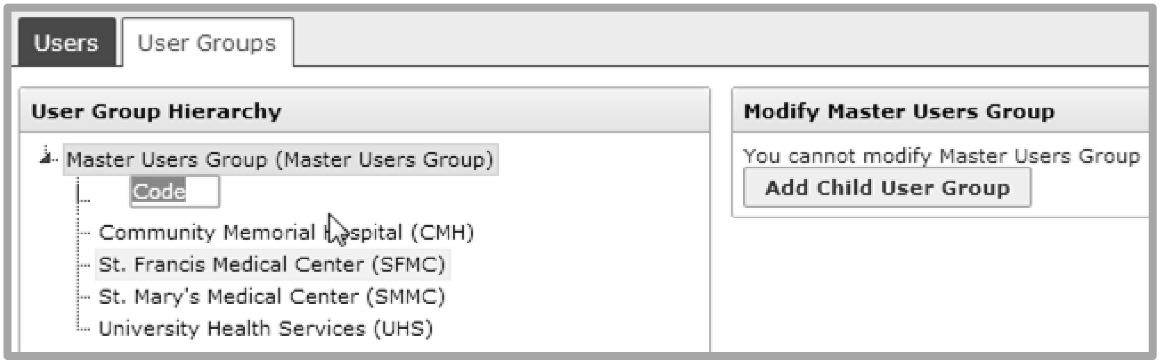
Adding a User Group

To add a new user group, select the appropriate parent group from the user groups tab. After selecting the appropriate parent user group, click the **Add Child User Group** button.

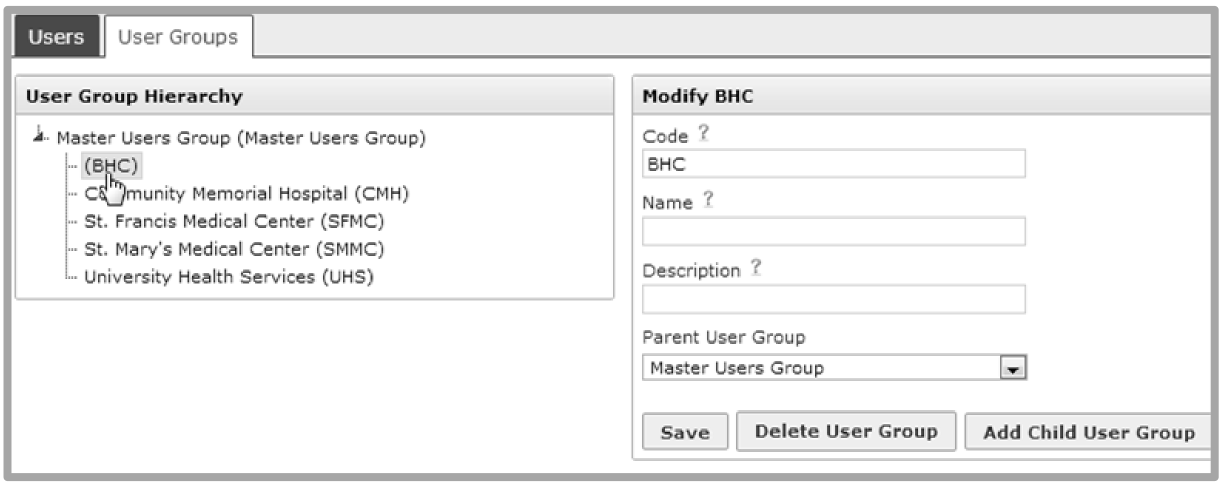
Note: The message "You cannot modify Master Users Group" means you are not able to edit or delete the top-level group, but it does not prevent you from adding a child user group.



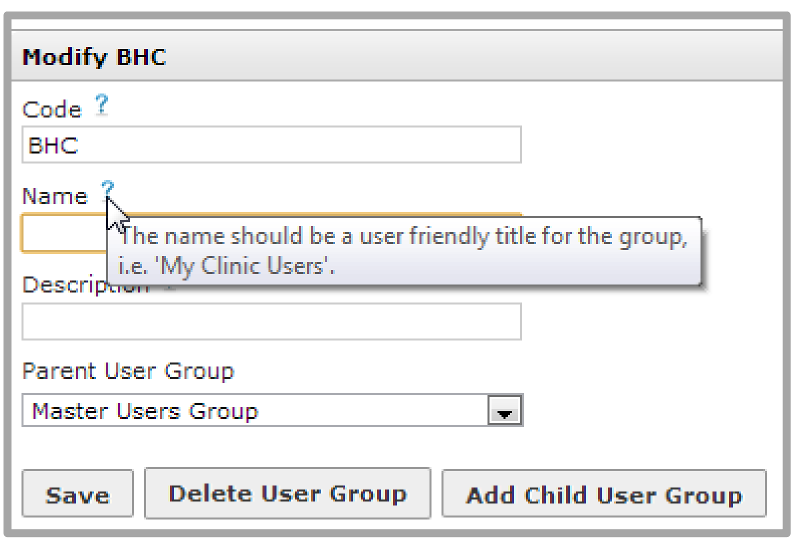
After clicking **Add Child User Group**, a new text box will appear in the panel on the left side with the word **Code** highlighted. Create an easily identifiable code or abbreviation for the user group and hit Enter. Departments or additional locations of an existing group should be added beneath this child group.



The new user group will appear at the top of the list in parentheses. To complete the setup, click on the name.



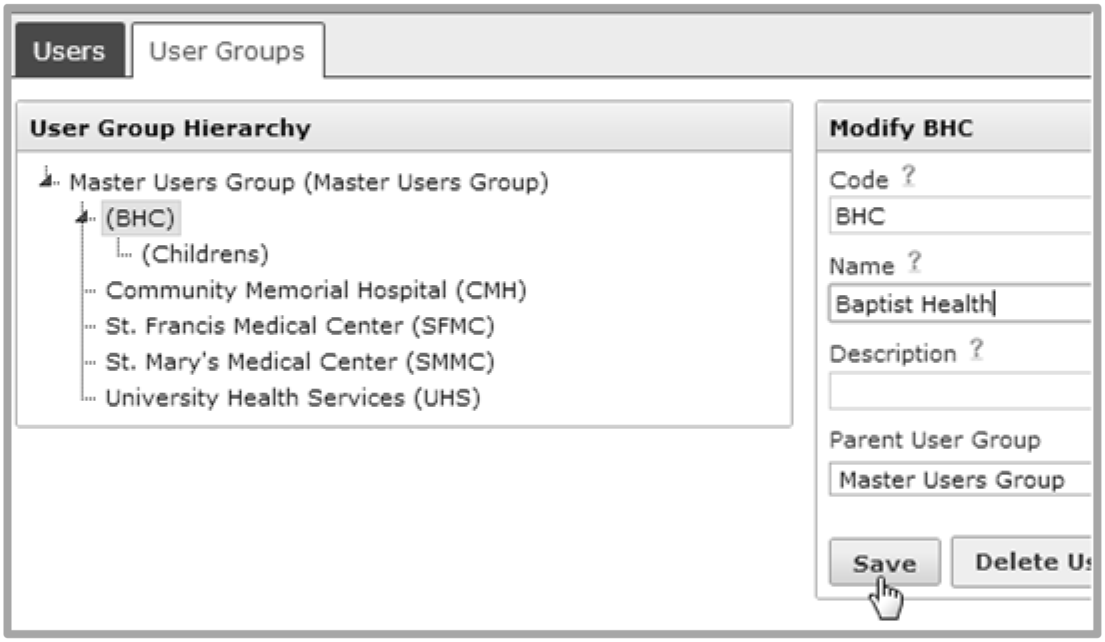
Tooltips will appear when hovering your cursor over the question mark by each field.



Edit all desired fields and click **Save**.

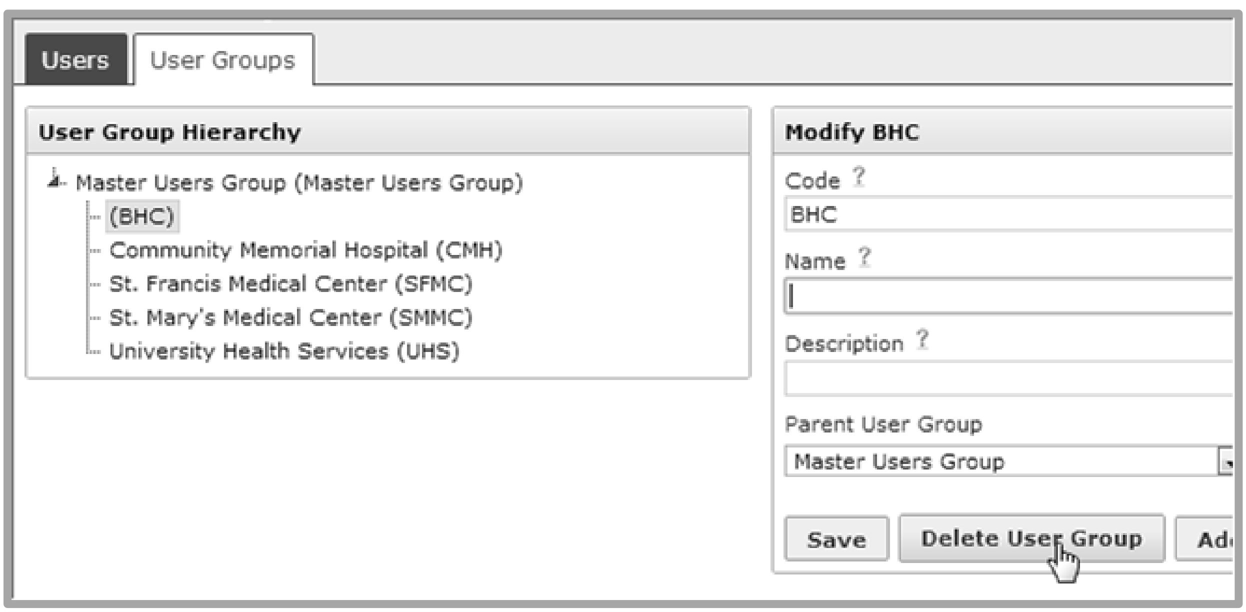
Editing a User Group

To edit an existing user group, select the group from the list, make your changes, and click **Save**. In the example below, information is being added to the *Name* field for the group with a *Code* of “BHC”.



Deleting a User Group

User groups with assigned users or child user groups may not be deleted. To delete a user group that does not have users or child user groups, select the user group and click the **Delete User Group** button.

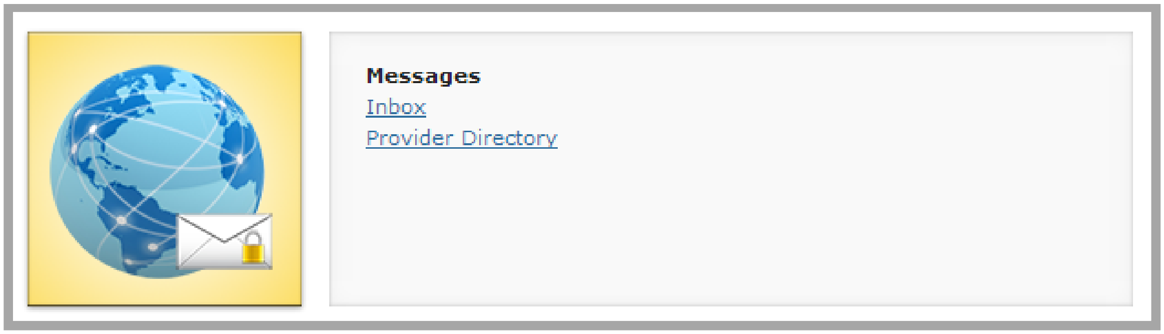


If the user group has assigned users or child user groups, the following message will appear:


Parent User Group
Master Users Group
Save
Delete User Group
Add Child User Group
The user group has child user groups or has user assigned to it.

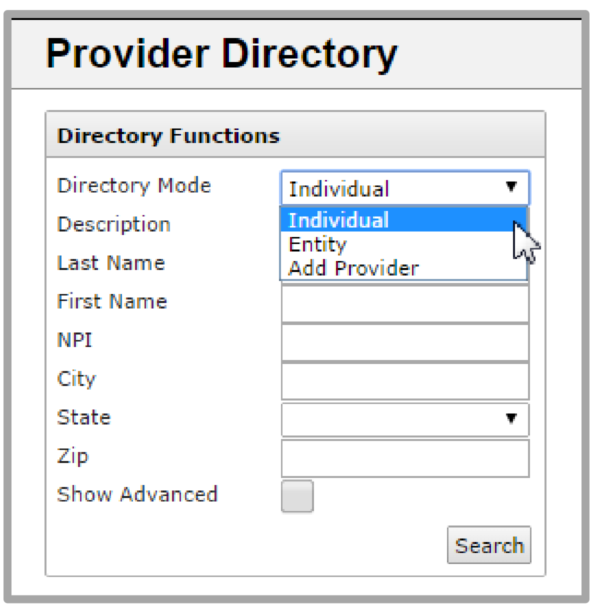
PROVIDER DIRECTORY

The Provider Directory allows you to search for providers within your own HIE and, in some cases, other exchanges.

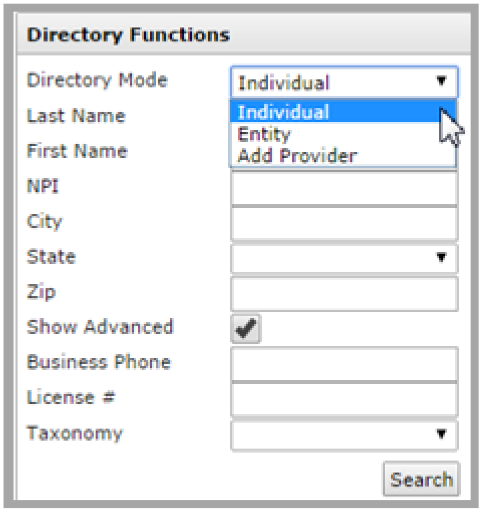


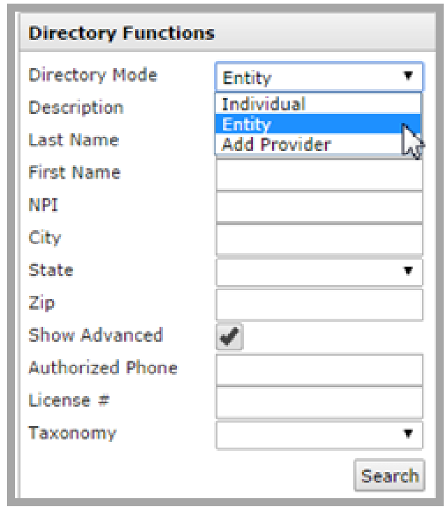
Searching the Provider Directory

Multiple options exist for searching the Provider Directory, including searching for both individuals and entities. To begin, select one of these options, either **Individual** or **Entity**, from the *Directory Mode* dropdown menu.



Enter information about the provider being searched for in the appropriate text boxes. Clicking on the *Show Advanced* check box will reveal additional search options.





In addition to standard demographic information, searches can be conducted using:

- **Description –** entity search only; search for an entity's name (e.g., Main Street Clinic) in the HIE database or in any linked databases
  Note: The results will include entities for which the name entered as the entity's description is an exact match to the search terms.
- **NPI –** National Provider Identifier; search using the individual or entity's 10-digit number from the NPI Registry, available from CMS
- **License #** – search for an individual or entity's professional license number
- **Taxonomy** – search for an individual or entity's practice category or specialty from options in the dropdown menu

Once the search information has been entered, click the **Search** button. Results will appear to the right of the search box. Select the desired individual provider or entity from the list of results by clicking on its result row.

Viewing and Editing Provider Information

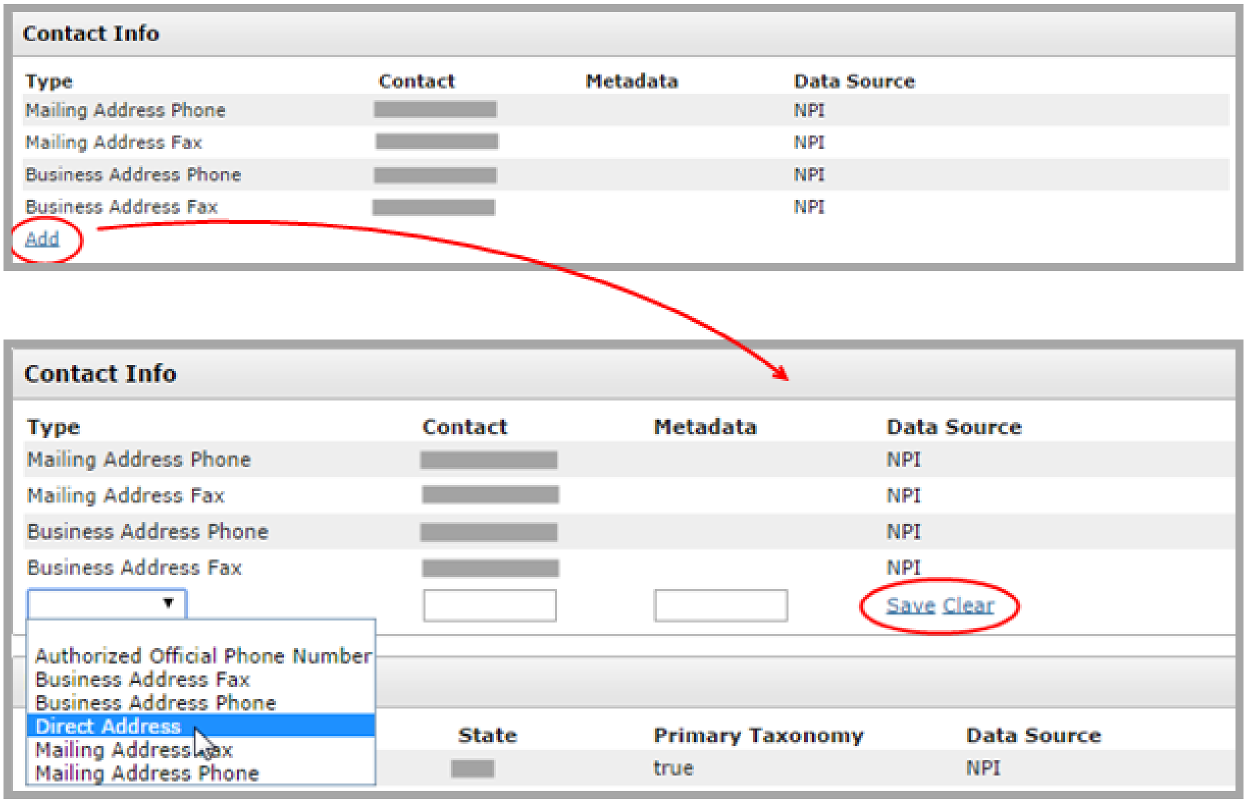
Once a provider is selected, the *Provider Detail* screen appears, showing the **View Individual Provider** tab (or for entities, the **View Entity Provider** tab).

On this screen, information about the provider is divided into a number of panels:

- **Names/Officials:** lists demographic info about a provider or each of an entity's officials
- **Identifiers:** lists ID numbers issued by NPI, Medicare, Medicaid, etc., and their effective dates
- **Addresses:** lists mailing addresses
- **Contact Info:** lists phone numbers, fax numbers, and Direct message addresses

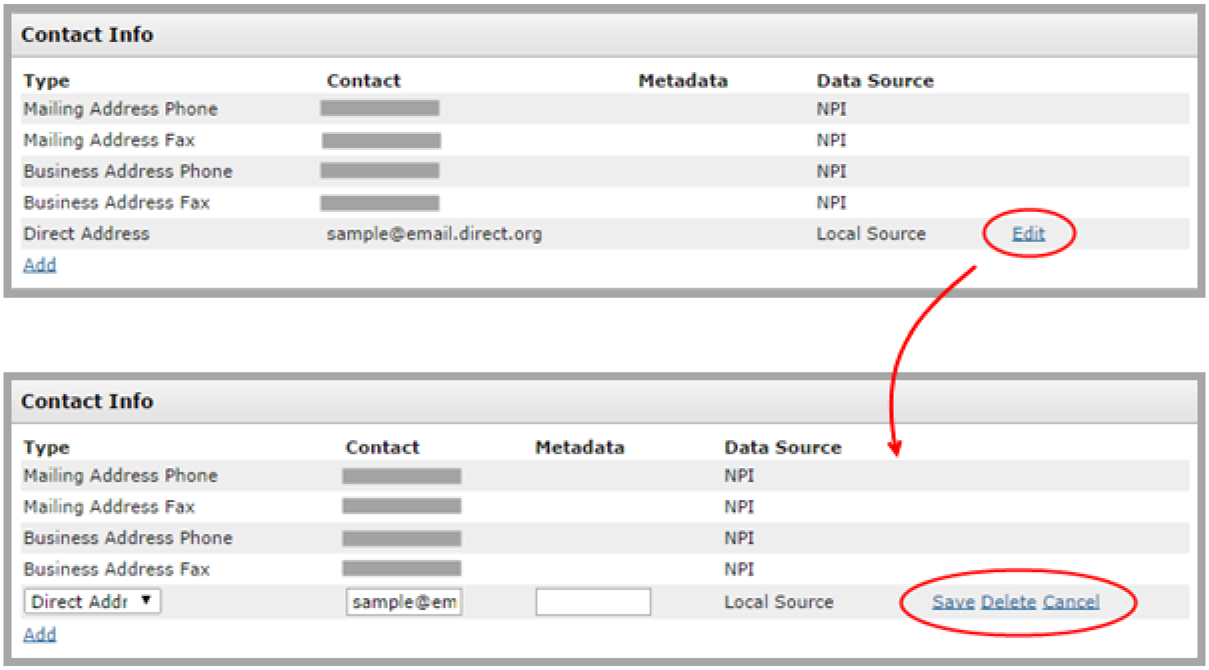
- **Licenses:** lists the numbers of any licenses held, the associated taxonomy classification, and their state of issuance
- **Descriptions (Entities only):** lists any specific identifying information about the entity

Additional information can be added to any of the above panels modified by clicking the **Add** link at the lower left of the appropriate panel. Fill in any boxes and make selections from dropdowns as appropriate.



When finished, click on the **Save** link to the far right of the row to save the changes, or click **Clear** to cancel the changes.

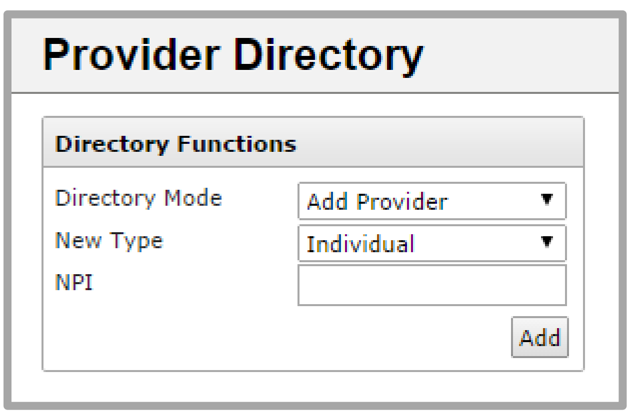
Any added information can be changed again by clicking on the **Edit** link that will appear next to user-added rows. Changes can be saved or cancelled, or the row can be removed completely by clicking the **Delete** link.



Note: Any manual additions made to provider information will appear with a data source of "Local Source", and will be visible to any user that has access to the Provider Directory.

Adding a New Provider

To add a new provider to the local Provider Directory, select the **Add Provider** option from the *Directory Mode* dropdown menu on the *Provider Directory* search page. Choose the appropriate provider type (Individual or Entity), and enter a valid 10-digit NPI number in the appropriate box.



Click the **Add** button and you will be directed to the **View Individual Provider** (or **View Entity Provider**) screen, where other information can be added.

MEANINGFUL USE

Meaningful Use Overview

Meaningful Use (or MU) refers to a set of objectives laid out by the Centers for Medicare & Medicaid Services (CMS) in their Medicare and Medicaid Electronic Health Record (EHR) Incentive Programs. The incentive program aims to encourage the "meaningful use" of electronic health records (EHRs) by healthcare providers.

Healthcare providers participating in the EHR Incentive Programs proceed through three different stages of MU over a specific timeline. Currently, only Stages 1 and 2 have been implemented; Stage 3 is set to begin in 2017. As MU stages increase, the requirements for meeting specific measures become more stringent.

Each objective has one or more associated measures for users of EHRs to achieve. For instance, the Patient-Specific Education objective requires healthcare providers to use clinically relevant information from Certified EHR Technology to identify patient-specific education resources and provide those resources to the patient.

Compliance with an objective's measure is determined by means of numerator reporting. CMS has defined numerators and denominators for each measure:

- Denominators define the total number of data points that are eligible to meet a measure's objective.
- Numerators define the number of data points that have met the objective's measure.

For example, the Patient Education measure defines its denominator and numerator as follows:

- The denominator is the number of unique patients admitted to the eligible hospital or seen by the eligible professional during the reporting period.
- The numerator is the number of patients in the denominator who were provided patient-specific education resources identified by the Certified EHR Technology.

Certain exclusions may also apply to certain measures.

For more information on Meaningful Use, please visit: http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html

Meaningful Use in the Web Client

The Unify™ Data Management Platform Web client provides a means of running on-demand reports to calculate compliance with MU objectives using information in the HIE's database.

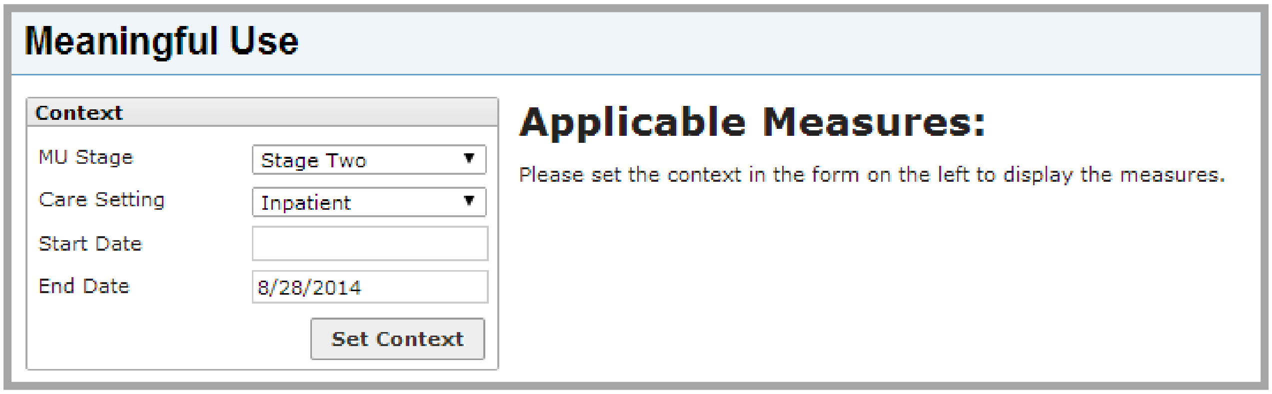
On the **Meaningful Use** screen, from the Web client's **Administration** menu, administrators can generate reports for various Meaningful Use Stage 1 and 2 measures.

The information generated in each report will represent only the actions or data points that qualify for the selected measure (numerator). These counts will need to be cross-referenced line-by-line with the cases and data points that qualify for the denominator, as obtained from the facility's EHR. Denominators are often the same across many measures (e.g., the number of unique patients discharged from the hospital during the EHR reporting period), and the EHR is the "source of truth" for admission and discharge information.

Note: In addition to on-demand numerator reports produced by the Web client, a recurring task can also be set up that will automatically run the report on a defined time interval and deposit the report to a defined location. Please contact your HIE Administrator for more information.

Generating Meaningful Use Reports

Reports for different measures can be created by selecting criteria in the *Context* box.



These criteria will set the scope of the reports. Each is discussed in more detail below:

MU Stage:

Select either **Stage One** or **Stage Two** from the dropdown. This will calculate the appropriate percentages for the stage selected.

Note: Reports are currently available for Meaningful Use Stages 1 and 2.

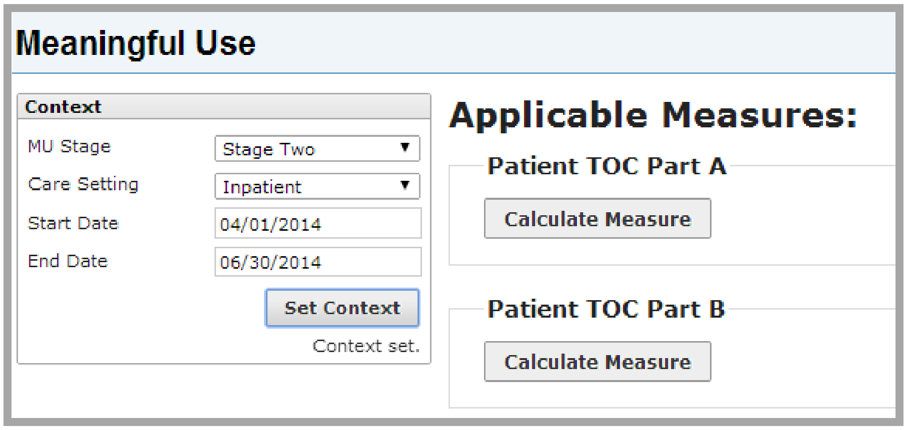
Care Setting:

The requirements for meeting MU measures often change based on whether care was provided in an ambulatory (i.e., outpatient) or inpatient setting. Choose either **Ambulatory** or **Inpatient** for the measure report, as appropriate.

Start Date/End Date:

Data for the Meaningful Use report will be pulled from the date ranges chosen in these fields. Either choose a date from the calendar widget, or type in the date in mm/dd/yyyy format.

Once all of the context parameters have been entered, click on the **Set Context** button. A small notification stating "*Context set.*" should appear briefly. A list of applicable measures will appear to the right of the *Context* box.



Applicable measures will differ depending on whether the context was set to MU Stage 1 or Stage 2 and on the selected care setting. Measures currently available include:

Incorporate Labs:

Percentage of numerical or postive/negative lab results included into a provider's EHR as structured data.

Patient VDT Part A:

Percentage of patients provided access to their electronic health information.

Patient VDT Part B:

Percentage of patients who view, download, or transmit their electronic health information.

Patient Specific Education:

Percentage of patients provided with patient-specific educational resources.

Patient TOC Part A:

Percentage of referrals or transitions of care from a provider that are accompanied by electronic summary of care documents for transferred patients

Patient TOC Part B (Stage 2 only):

Percentage of electronic summary of care documents which are transmitted either using Certified EHR Technology, or using an HIE which is an eHealth Exchange participant.

Patient Reminders (Ambulatory care setting only):

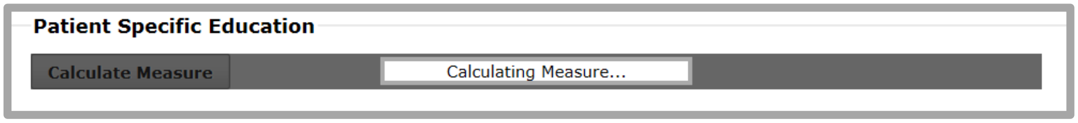
Percentage of patients sent reminders for preventative or follow up care

Secure Electronic Messaging (Stage 2 only, Ambulatory care setting only):

Percentage of secure electronic messages sent by patients and received by healthcare providers.

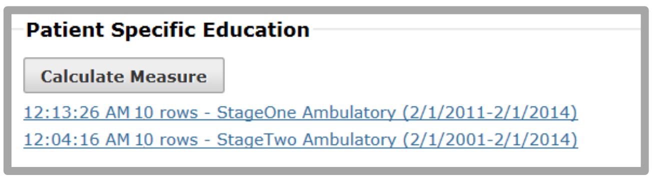
The most common use of the MU numerator reports will be for the TOC and VDT objectives.

To generate a calculation for a specific measure, click on the **Calculate Measure** button present under a measure title. A status bar will appear as the calculation is generated.



Once the calculation is complete, a link will appear for each calculation report that was generated. Reports that have previously been generated will remain available for the duration of the current session. Each link's text describes the context details for the measure calculation, including:

- the time and date the report was generated
- the number of rows of relevant data points
- the context's Meaningful Use Stage
- the context's Care Setting
- the context's start and end dates



Numerator report files are created in a comma-separated values (.csv) format. Clicking on a link will begin download of a report file.

Depending on your computer's settings, the file may immediately open in a browser window. If not, it can be opened by a spreadsheet program such as Microsoft Excel.

Transitions of Care

The Transitions of Care (TOC) objective is one of the most applicable of the MU Stage 2 objectives for an HIE. The objective requires that providers who refer or transition their patients to another care setting provide a summary care record for each referral or transition of care.

Three individual measures are associated with the TOC objective; however, only measures 1 and 2 have numerators that can be calculated:

- Measure 1 (referred to above as TOC Part A) requires that a summary care record be provided for greater than 50% of all referrals and transitions of care. The numerator report would include all instances where a Summary of Care CCDA was transmitted, downloaded, or printed within the selected date range.

  Note: The facility may choose, at their discretion, to include CCDAs that were generated outside of the Unify™ Data Management Platform, in combination with or in lieu of this report as applicable.

- Measure 2 (referred to above as TOC Part B) requires that the summary care record be transmitted electronically using certified technology for greater than 10% of all referrals and transitions of care. The numerator report would include all instances where a Summary of Care CCDA was transmitted within the selected date range, using any of the certified transport methods (Direct, XDR/XDM, and SOAP).

  The report's algorithm is configured to identify specific attachment types, as defined by the client. For instance, TOC documents may be termed "Patient Summary" at one facility or "Summary of

Care" at another. The algorithm would identify all applicable transmissions to be included in the report.

- For both measures 1 and 2, the denominator, obtained from the facility's EHR, is the number of transitions of care and referrals during the EHR reporting period. The numerator report obtained from the Unify™ Data Management Platform includes all transmissions of the Summary of Care CCDA, some of which may not correspond to a transition of care or referral. By cross-referencing the denominator list with the numerator report, the facility can determine the actual number of transitions of care and referrals for which a summary of care record was either provided (measure 1) or transmitted via one of the certified methods (measure 2).

View, Download, Transmit

The view, download, transmit (VDT) objective is another MU Stage 2 objective that is relevant to an HIE. This objective requires that patients be given the opportunity to view online, download, and transmit their health information to a third party.

Both measures associated with the VDT objective have numerators that can be calculated by the Unify™ Data Management Platform:

- Measure 1 (referred to above as VDT Part A) requires that greater than 50% of patients discharged from the hospital or seen by the eligible professional (EP) have their information available online.

  Inpatient numerator report includes all patient records that meet these criteria:

  - Linked to a Patient Portal user account within 36 hours of discharge
  - Both an Inpatient Summary CCDA and TOC CCDA were present within 36 hours of discharge

  Ambulatory numerator report includes all patient records that meet these criteria:

  - Linked to a Patient Portal user account within 4 days of the date that an Ambulatory Summary CCDA was created

- Measure 2 (referred to above as VDT Part B) requires that greater than 5% of patients discharged from the hospital or seen by the EP either view, download, or transmit their information to a third party.

  The numerator report would include all patient records for which a linked user account (either the patient or an authorized representative) logged in to the Patient Portal within the selected date range to view, download, or transmit any part of the record

Note: The numerator reports for these measures are only available to clients that have implemented the platform's Patient Portal for use by their patients.

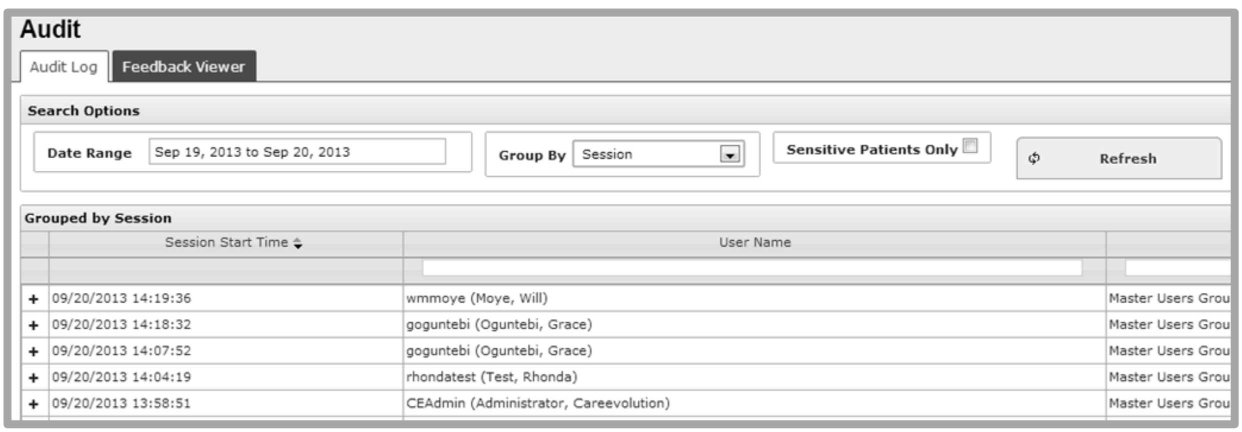
TRUVEN HEALTH ANALYTICS

AUDIT & FEEDBACK

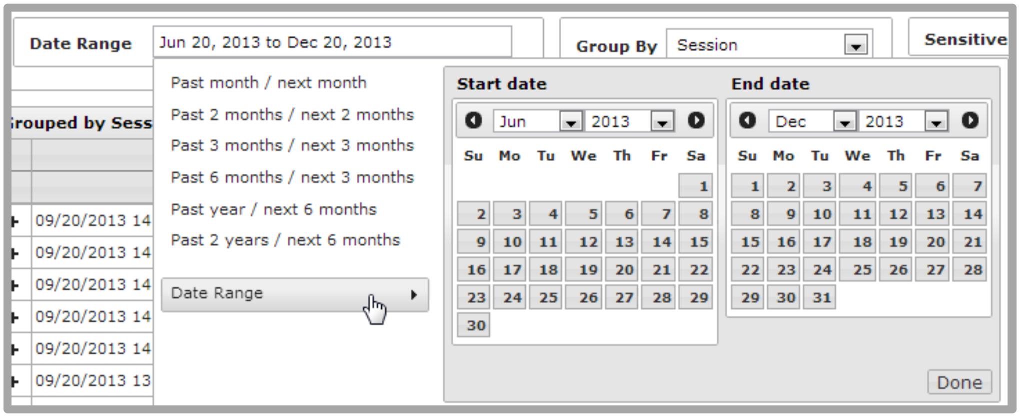
The Audit & Feedback screens allow administrators to view system activity and provide user support.

Audit Log

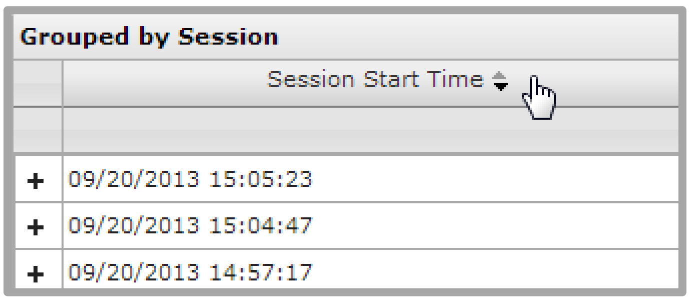
The Audit Log provides access to a record of all user activity, including Session Start Time, User Name, and User Group when grouped by session; if grouped by user, it contains User Name, User Group, Address, and Phone Number.



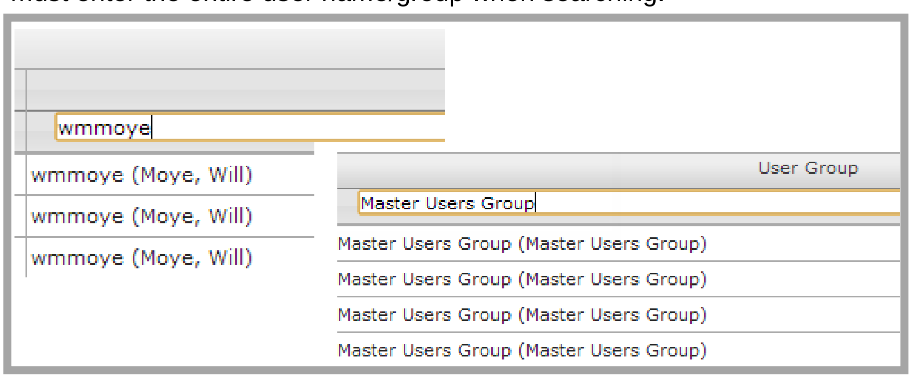
By default, the search start date is set to the previous day and the end date to the current day. Results are grouped by session. Clicking on the *Date Range* filter allows you to limit the results to any of the displayed ranges or to specify a different start and end date.



To sort by Session Start Time, click on the column header.

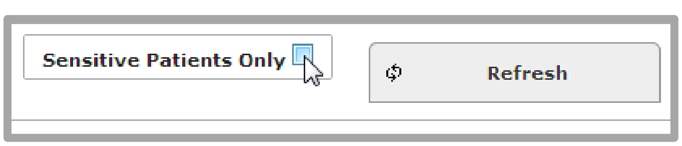


Search by user name or user group using the search boxes above the respective columns. Note: You must enter the entire user name/group when searching.

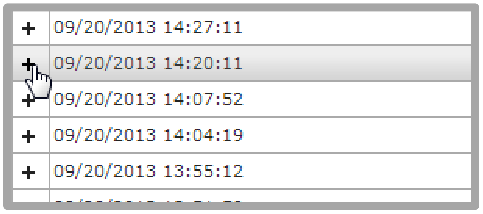


To filter by users who have viewed sensitive records, select the *Sensitive Patients Only* checkbox and then click the **Refresh** button. To return to the previous view, uncheck the box and click **Refresh** again.

Note: Only users who have been assigned a sensitive health role can view records marked as sensitive.

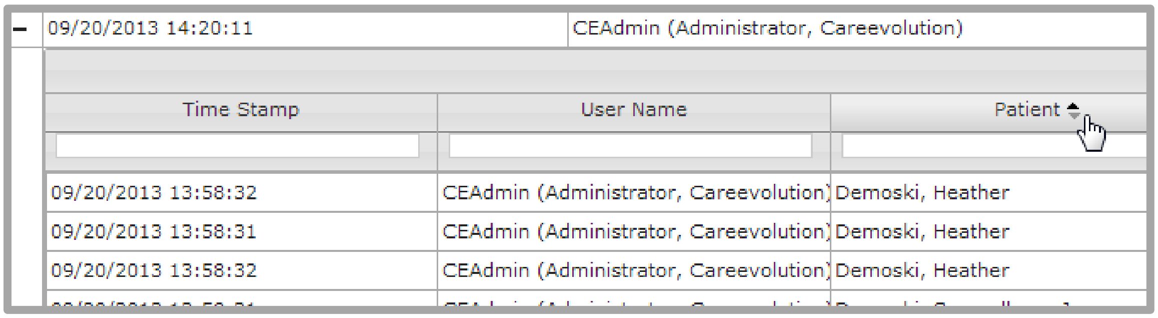


Click on the **+** sign beside the session to view the details of an event.



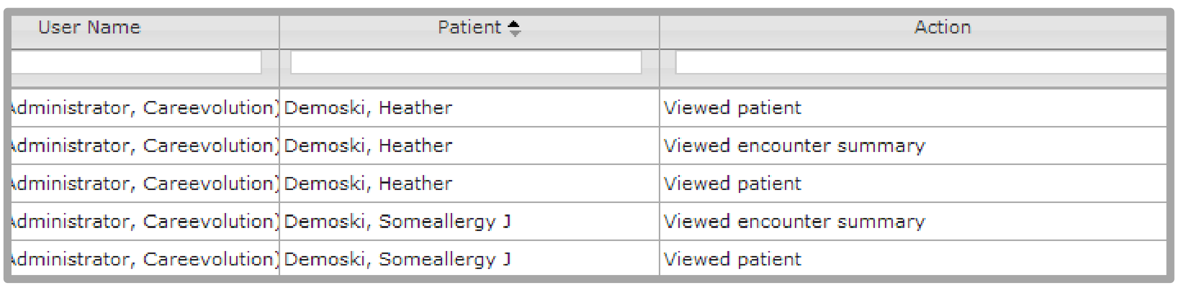
+	09/20/2013 14:27:11
+	09/20/2013 14:20:11
+	09/20/2013 14:07:52
+	09/20/2013 14:04:19
+	09/20/2013 13:55:12

Click on any of the headers to sort by column.



Time Stamp	User Name	Patient
09/20/2013 13:58:32	CEAdmin (Administrator, Careevolution)	Demoski, Heather
09/20/2013 13:58:31	CEAdmin (Administrator, Careevolution)	Demoski, Heather
09/20/2013 13:58:32	CEAdmin (Administrator, Careevolution)	Demoski, Heather

Each log event includes session start time, user name, patient viewed, actions performed by the user, details (including page duration), and applications viewed.



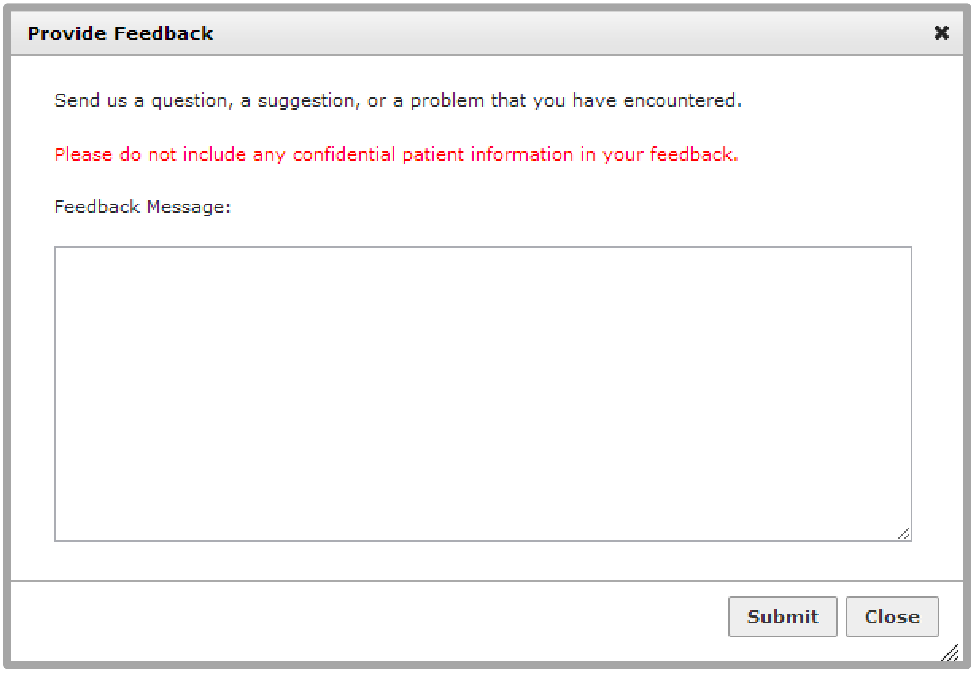
User Name	Patient	Action
Administrator, Careevolution)	Demoski, Heather	Viewed patient
Administrator, Careevolution)	Demoski, Heather	Viewed encounter summary
Administrator, Careevolution)	Demoski, Heather	Viewed patient
Administrator, Careevolution)	Demoski, Someallergy J	Viewed encounter summary
Administrator, Careevolution)	Demoski, Someallergy J	Viewed patient

Feedback Viewer

The functionality available on the **Feedback Viewer** screen allows administrative users to receive messages about the system from other users. These messages provide a forum for users to ask questions, report problems, or offer suggestions regarding use of the Web client and the HIE system.

Each screen of the Web client includes a **Provide Feedback** link in the upper right-hand corner.

Once a user clicks on the **Provide Feedback** link, a feedback message window will appear.



Each message will automatically include information about the page and/or patient currently being viewed by the submitting user. The user should not include patient demographics or other identifying information in the body of the message**.**

Administrative users with the appropriate rights will be able to browse all feedback using the **Feedback Viewer**. Feedback messages can be filtered by date range, user ID, keyword, or Web page name, using the Filter Feedback section on the left side of the screen.

Once a filter is applied, a table of matching feedback messages will be generated to the right. Each message listing includes a timestamp, the Web address identifying the page about which feedback was left, any message from the submitting user, the submitting user's login and name, and associated patient information, such as MRN.