Solution Center Administrator Guide

Solution Center Overview

The GLHC Solution Center provides access to the GLHC Inbox and the Virtual Integrated Patient Record (VIPR). The GLHC Inbox stores and organizes test results and Admit, Discharge, Transfer notifications for your patients. The Virtual Integrated Patient Record (VIPR) is a longitudinal community health record that organizes the clinical information of over 10 million patients. Healthcare organizations across the state and the Midwest contribute the health information in real time.

Solution Center URL Link

https://hie.gl-hc.org/ccv/

Organization Administrator (Org Admin) Overview

Protecting patient information is a top priority as GLHC collaborates with healthcare providers to improve health outcomes and healthcare value for patients. GLHC follows all Michigan and Federal laws when storing, organizing, and sharing health information. Those who use the Solution Center are subject to strict privacy laws under HIPAA and must have a Treatment, Payment, or Operations (TPO) relationship with the patient.

The role of the Organization Administrator (Org Admin) is a vital role for the organization using the Solution Center. Each organization needs to have at least one staff member designated as an Org Admin. The GLHC Implementation Consultant (IC) will work with someone in a leadership role within the organization to determine the appropriate person.

Org Admin responsibilities:

- Confirm that all users are actively employed at their organization.
- Create and manage all users for the organization.
- Deactivate users when a staff changes their role, should not have access, or is terminated from employment.

To add an additional Org Admin, the current Org Admin needs to email or call GLHC Support. The email must include:

- The name and address of the organization
- New Org Admin requested User ID
- Full Name
- Email address
- Phone Number
- Additional User roles (for VIPR or Inbox) held by the Org Admin

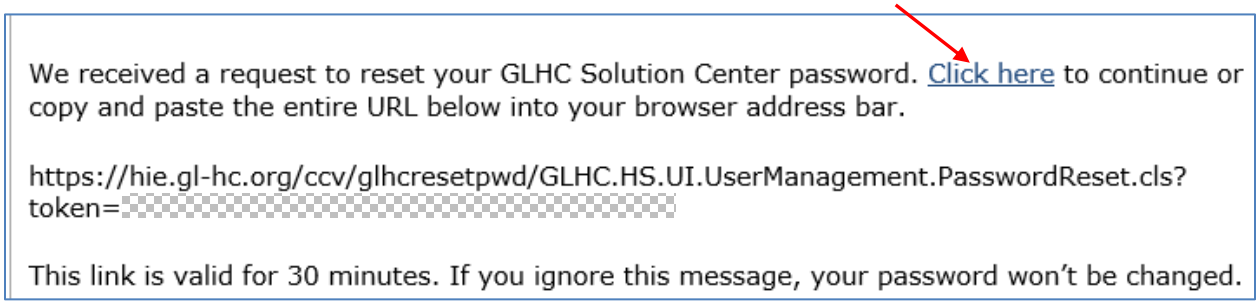
If the Org Admin has left the organization before requesting the creation of the new Org Admin, a person of leadership with the organization must contact their GLHC Implementation Consultant who will make the request for a new Org Admin.

Important information

- Every Solution Center account must be assigned to one individual. Shared accounts are not allowed.
- Accounts are for employed staff of an assigned facility.
- When creating a user, select the Facility BEFORE selecting the role.
- Admins will need to review all of their users with access and verify the appropriateness of each user's role every 90 days. Any changes needed should be made immediately following the review.
- Passwords must be at least eight characters in length and contain at least three of the following four types of character: uppercase, lowercase, number, non-alphanumeric.
- Passwords periodically expire.
- Sessions will log out after a period of non-activity
- Inactive accounts are disabled after a period of inactivity

Initial Login for Org Admin

1. Admins will receive the following email when their account is activated by GLHC Support. Select either **Click here** or copy the link into your internet browser.

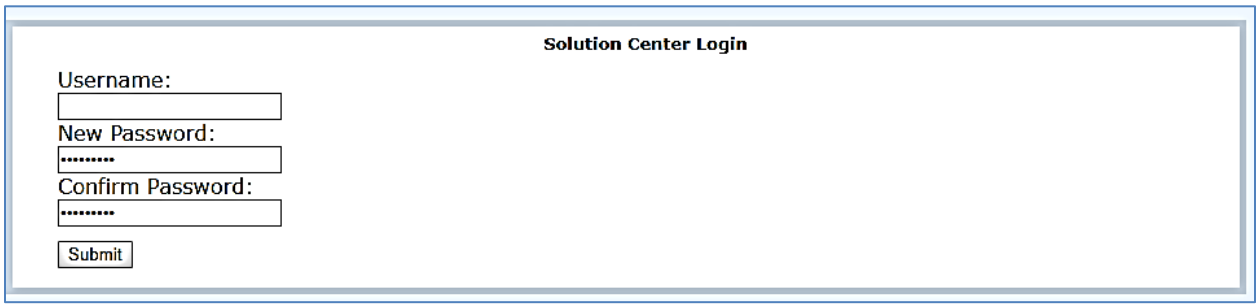

We received a request to reset your GLHC Solution Center password. Click here to continue or copy and paste the entire URL below into your browser address bar.

https://hie.gl-hc.org/ccv/glhcresetpwd/GLHC.HS.UI.UserManagement.PasswordReset.cls?token=

This link is valid for 30 minutes. If you ignore this message, your password won't be changed.

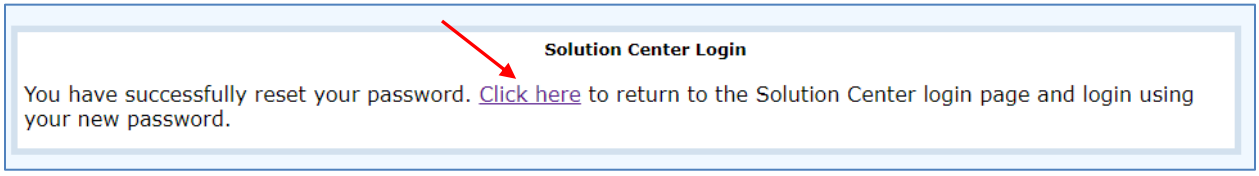
Important: The link to reset the password is valid for 30 minutes. Contact GLHC Support to resend the request if you are unable to access the email and reset your User Account password within this timeframe.

2. The first screen you will see after navigating to the Solution Center is below:

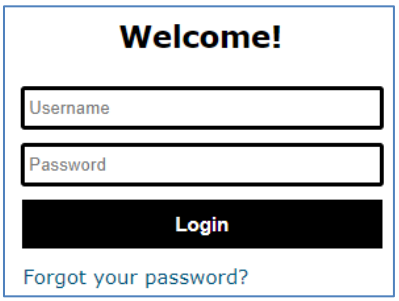


3. Enter your Username provided by GLHC Support and then create and confirm a New Password. Click **Submit** when finished. Contact GLHC Support if you did not receive your Username.

4. Click on the **Click here** link to return to the Solution Center login page.



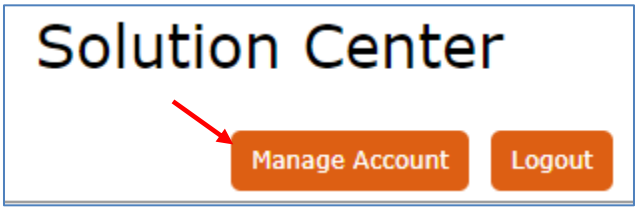
5. Re-enter your Username and password, click **Login.**



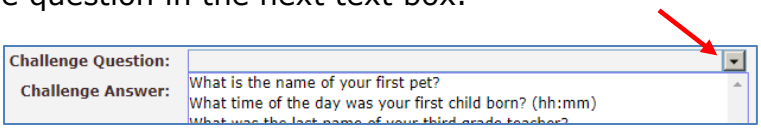
Creating a Challenge Question and Answer

It is very important to select a Challenge Question and enter a Challenge Answer. GLHC Support will not be able to assist you without this information. You will need to successfully answer your challenge question when calling GLHC Support for assistance.

1. Click on the "Manage Account" icon in the upper right-hand corner of the Solution Center screen.

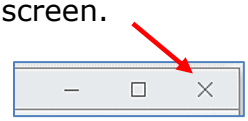


2. Select the dropdown arrow for **Challenge Question** to display the options. Answer the question in the next text box.



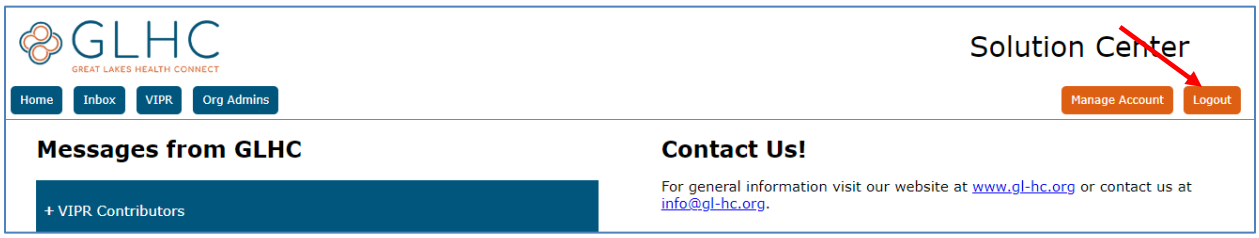
3. Once you have completed your question and answer, click **Save Account**. The orange **Account Saved** button will confirm that your Challenge Question and Answer have saved to your account.

4. Exit out of the **My Account** screen by clicking the **x** in the upper right hand corner of the **My Account** screen.



Logging Out

For security reasons, log out of the Solution Center when you are no longer using the tool. Logging out is not the same as exiting out of the application. To log out, click **Logout** button.

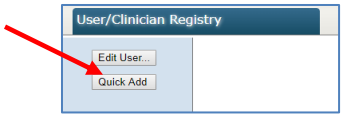


Creating a User Account

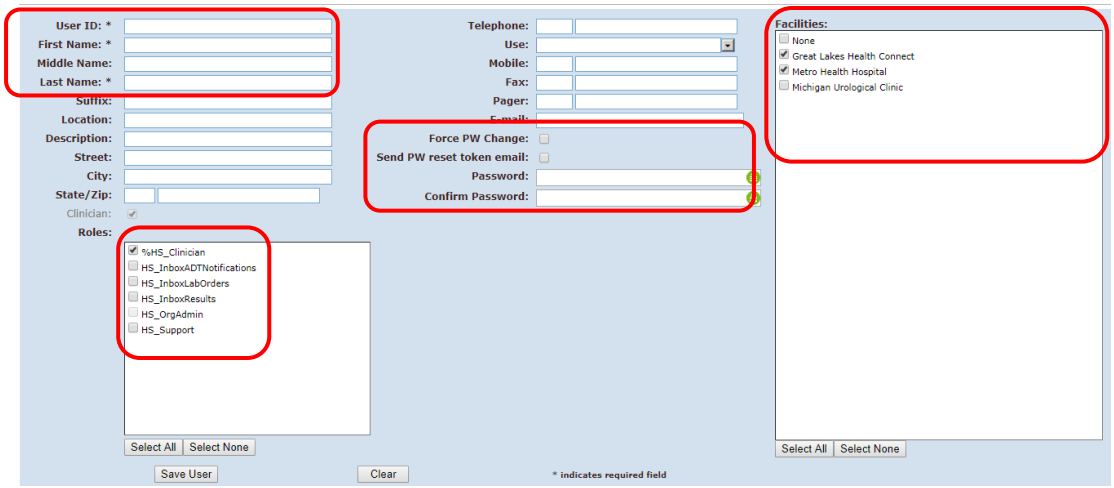
It is important to follow each step to ensure that Users have proper access information within the Solution Center. User identities must be verified prior to creating accounts. Accounts should only be created for employed staff within your organization.

1. Navigate to the Solution Center and then click the **Org Admins** button.

2. Click **Quick Add**.



3. Enter all mandatory information.



Field Descriptions:

a. **User ID:** This field becomes the Username and is unique in the Solution Center. It is important to let the User know of the created User ID as they will need this upon initial login. A message will display if the User ID is already being used by another User. You will be prompted to create a different ID.

b. **First Name:** User's first name

c. **Last Name:** User's last name

d. **E-mail:** Only required for Users who wish to reset their own password.

e. **Password:** This field allows Org Admin to create a temporary password for the User. This is an alternative to using the user's email address to reset their own password. Do not enter a password if an email is provided. You must, however, add a temporary password if you are not adding an email to the account.

f. **Send PW reset token email:** By checking the box an email will be sent to the user with instructions for resetting their Solution Center password.

   Important: This checkbox should only be used if a User has an email added to their Solution Center profile. When checking this box, always ensure "Force PW Change" is NOT checked

g. **Facility:** All organizations sending or accessing data to the Solution Center are called "facilities". This field will list facilities that your account, is affiliated with. If more than one facility is listed, select the applicable Facility/Facilities for the user to be affiliated with. (You may select multiple facilities)

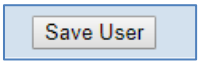
   Important: Select the Facility prior to selecting the Role (next field).

   - Contact GLHC Support if a Facility is missing from the list.

h. **Roles:** The user's role determines the level of access the user will have to information within the Solution Center. These different levels of interaction are organized into "roles" and it is mandatory that you select at least one for each user. Select the role most appropriate with the user's job function and responsibilities (see "Role Options" for more information). A user can have one role for VIPR and multiple roles for Inbox if applicable.

   - Only applicable roles for your organization will display under this section. If you believe that your organization should have other listed roles, please contact your Implementation Consultant to discuss adding these roles. They will work with GLHC Support to get them added.

   - Once roles are selected, click **Save User.**



VIPR User Roles

There are four VIPR user roles. Each user should have only one VIPR role.

1. **Clinical** - User will be able to view all data in VIPR.
2. **Clerical** - User will only see patient demographic, encounter, and insurance information.
3. **ACD** - User will only see Advance Care Directive (ACD) documents, patient demographics, and Patient Care Documents. No other result data will be available for view.
4. **Support -** This role is the most restrictive. This role allows the user to ONLY view patient information in VIPR that their own organization has contributed.

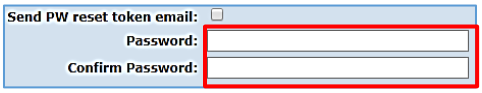
Inbox User Roles

There are two Inbox user roles. Users can have one or both Inbox roles.

1. **Results**- User will be able to view all test results from hospitals sending to the Inbox.
2. **ADT** - User will be able to view Admit, Discharge and Transfer (ADT) notifications, if available.

Creating/Resetting Password for Users without an Email Address

If the user does not have an email address or the 30 minutes timeframe is not practical, the Org Admin will need to create and confirm a temporary password within the user's account.



Do not use the "Send PW reset token email" checkbox.

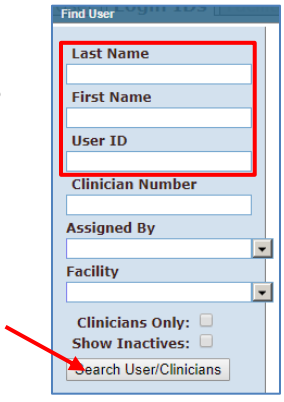
After creating and saving the temporary password, the Org Admin needs to communicate the Solution Center **URL**, **User Name,** and the **temporary password** information directly to the User in a confidential manner.

Managing Users

Org Admin manage users within their organization. This includes editing the User's first and last name, inactivating the account, unlocking the account, and managing passwords and roles. All modifications are made through the **Edit User** button.

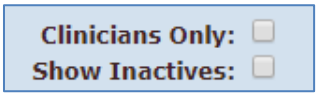
Searching for Users

1. Enter one or more of the following: User's **Last Name**, User's **First Name**, or **User ID**.
    a. Do not use **Clinician Number, Assigned By,** or **Facility** in your search criteria
    b. To locate all users for an organization, leave all fields blank.
    c. Only ACTIVE users will display
2. Click **Search User/Clinicians** button.



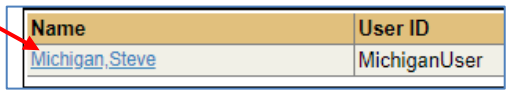
Filter the list of users:

- Search for Clinicians only
- Include inactive accounts in the search results



Editing a User Account

To edit a User click their Name (underlined in blue).



The screen below will display:

User Tab

In the **User** tab, any information that is not greyed out can be modified.

Common fields to edit:

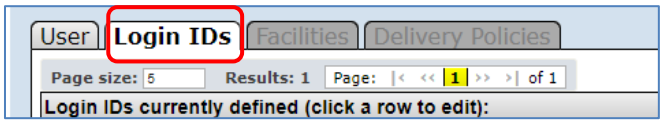
- First Name
- Last Name
- Email
- Active (box checked) **Note:** If box is unchecked, the User is inactive.

The **User ID** cannot be edited. A new account must be created if the User ID needs be changed.

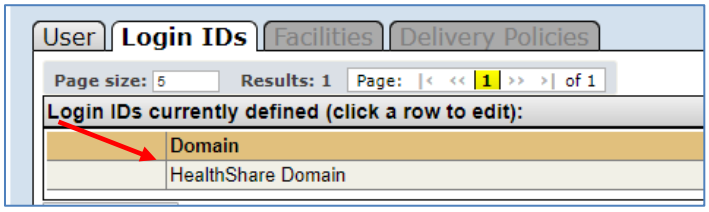
Click **Save User** after any changes are made to this page.

Login IDs Tab

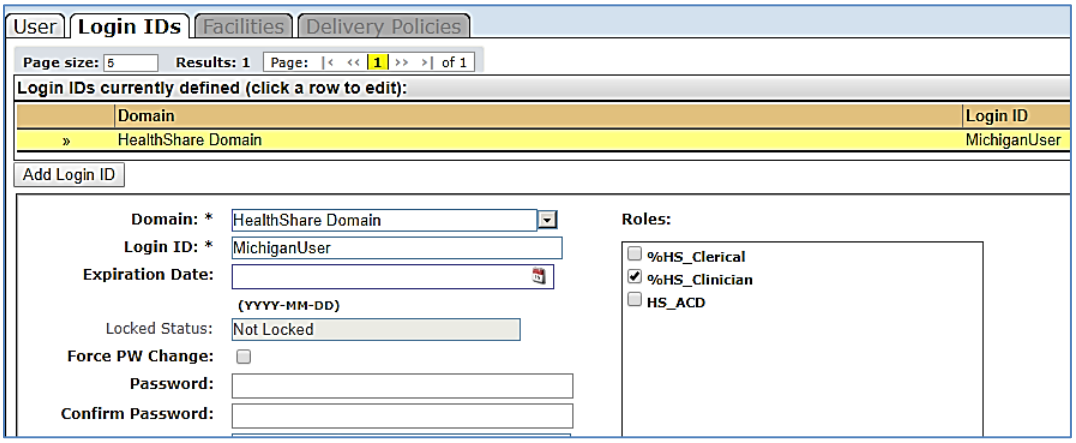
1. Select the Login IDs tab to modify a User's Password, Locked Status, Expiration Date, Challenge information, or Roles.



2. Click **HealthShare Domain** text in the **Domain** column.



3. The following screen will display:



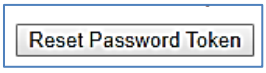
Only the subsequent information can be modified in this page:

- Adding an **Expiration Date** for accounts with a known expiration. Leave blank for accounts with no expiration.
- **Force Password Change** checkbox
- Enter a **Password** to be used as a temporary password
  - This includes **Confirm Password**
- The User's **Role**

Do not take the following actions!

- Click **Add Login ID**
- Modify/change the **Login ID**
- Delete **HealthShare Domain**

The **Reset Password Token** button will send the User an email containing a link for them to reset their password.



Once all changes are made select **Save Login ID** on this page.

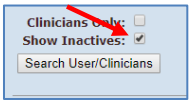
Inactivating a User Account

When an individual no longer needs access to the Solution Center, their account should be promptly inactivated. To inactivate an account unselect the **Active** box in the **User** tab and then click **Save User**.

The user will get an error message of **Login failed!** if they attempt to log in.

Reactivating a User Account

To reactivate an account:



1. Click the **Show Inactives** checkbox when searching for the user.
2. Inactive Users will not have an "X" in the **Active** column.

3. Select the User you wish to reactivate.
3. From the User tab, click the **Active** checkbox and then click **Save User**.

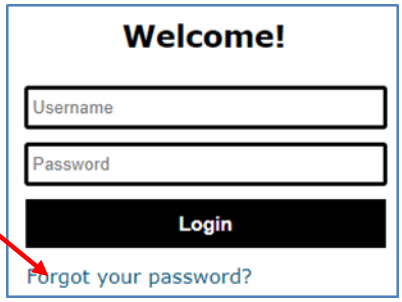
4. **Important:** You must click the **Active** checkbox and click **Save User** before you use the "reset password token". Otherwise the user will receive an error message of **Login failed!** when they attempt to log in after resetting their password.

Unlocking a User Account

After several unsuccessful login attempts, a user's account will be locked. A password change is required to unlock an account.

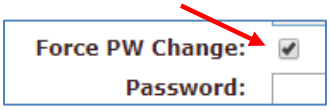
Accounts with an Email

To unlock an account that has an email, instruct the User to utilize the "**Forgot Password?"** link under the Login icon in the Solution Center to change their password which will unlock their account.



Accounts without an Email

1. Open the User's Account.
2. Go to the **Login IDs** tab and click **Force PW Change**.



3. Enter new temporary **Password** and **Confirm Password.**
4. Click **Save Login ID.**
5. Inform the User of the temporary password in a confidential manner and request that they log in as soon as possible to create their own password.