Creating and Managing User IDs

Great Lakes Health Connect (GLHC) provides each office the ability to create and manage users within the Command Center. This provision is only available to Command Center Administrators. This role is limited to a maximum of two people within each Command Center: Typically the administrators are the Practice Manager and one other designated person. This Quick Reference Guide will walk the user through creating and managing user IDs.

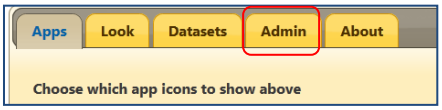
Note: It is the on-site Administrator's responsibility to manage the list of users and deactivate accounts when a user should no longer have access to the Command Center.

Accessing the Administration section in the Command Center

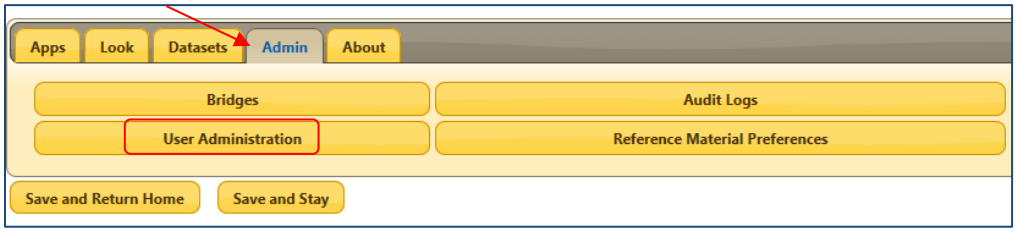
1. Log in to the **GLHC Command Center**.

2. In the top right corner, click on the "**Preferences"** icon.

3. Select the **Admin** tab

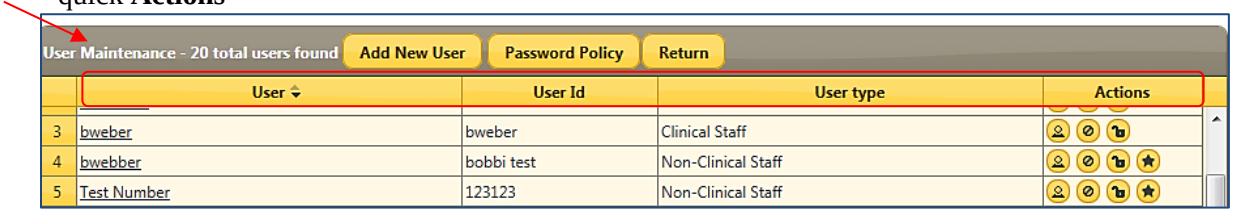


4. Select the **Admin** tab and then **User Administration**



5. The **User Administration** section provides the ability to add or inactivate new users as well as modify their level of access to the Command Center. It also allows the administrator to modify the Password criteria (to be explained later).

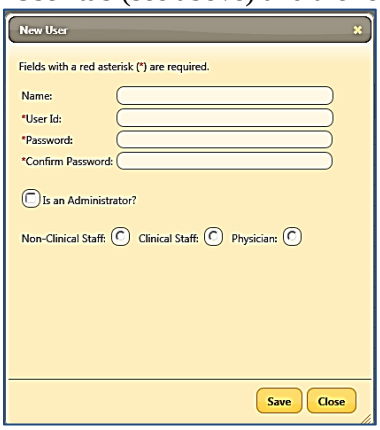
6. The **User Maintenance** worklist displays the **User** name, the **User ID**, the **User Type** and available quick **Actions**



Adding a New User

Note: Once you create a User ID, you cannot delete or change the ID. You may change the person's name (i.e. change of last name, etc.) **but if you need to change their ID, you must de-activate the current ID and then create a new ID for the person.**

To add a new user, select the **Add New User** tab (see above) and the following will display:



1. Enter the following:
    a. Name: Staff's First and Last Name
    b. User Id: Does not need special characters. (User ID's are NOT case sensitive)
    c. Password: Must be at least **6 characters** in length. (Passwords **ARE** case sensitive)
    d. Confirm Password: by retyping the desired password.
    e. Only select **Is an Administrator?** for Users with Administrative rights (1 – 2 per site)
    f. Select level of Command Center access. ** The majority of Command Center users are **Clinical Staff** (See next section for descriptions of Access Levels)

2. Select **Save**

Command Center Access Levels

There are 4 levels of access:

8	Steve Spieker	spiesd	Administrator - Clinical Staff	
9	Sam Dietzman	sam09126	Clinical Staff	
10	Mitch Kelly	kellmc	Physician	
11	Julie Klausing	klaujl	Non-Clinical Staff	

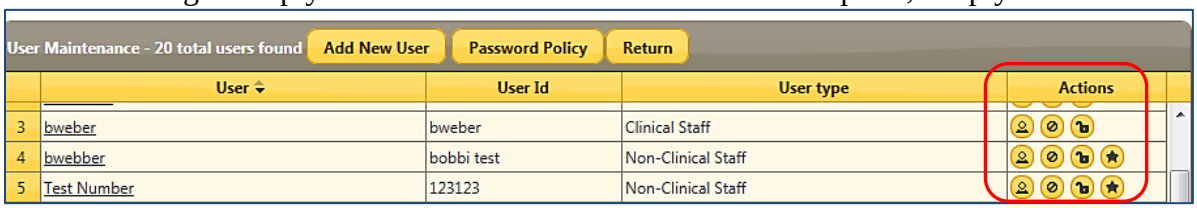
1. **Administrator** (**MUST** have an **Access Agreement** on file with Michigan Health Connect)
    a. Has access to the Admin tab
    b. Create new user accounts
    c. Inactivate expired user accounts
    d. Reset locked accounts
    e. Make changes to practice-wide Command Center settings
    f. Grant emergency PHI information access to non-clinical users
    g. Access to manage the Referrals Homepage
    h. Access to Folders and Rules within the Advanced View of the iNBox
    i. Has the ability to create new patients
    j. Has access to all patient drawers within the Patient Record

2. **Clinical Staff**
    a. Has the ability to create new patients
    b. Has access to all patient drawers within the Patient Record
3. **Physicians**
    a. Has the ability to create new patients
    b. Has access to all patient drawers within the Patient Record
4. **Non-Clinical Staff**
    a. Is unable to create new patients
    b. Has limited access to the Patient Record (Patient Demographics, Supporting Parties, Insurance and Patient Reminders)

Available Actions directly within the User Maintenance screen:

The User Maintenance screen allows the administrator to change several frequently-used settings for multiple users from a single screen **without having to open the User's record**.

To make changes simply click on the desired icon. To reset the option, simply re-click the icon.



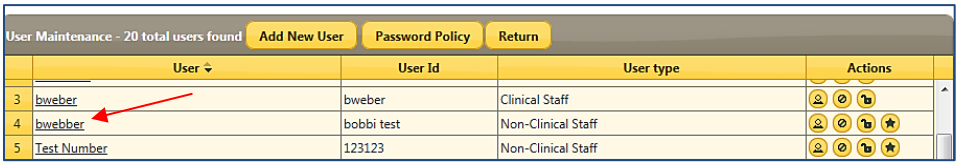
1. Make the user as Administrator **(only 2 active Administrators per office)**
2. Inactivate the user account. To be selected when the User is no longer using the Command Center or is no longer employed at the practice/facility.
3. Unlocking (or locking) the user account. To be selected when a User locks out their account.
4. Emergency access (for Non-Clinical Staff Only to be explained in page 5 of the Guide)

Action Buttons (Active / Inactive)	Description
	Administrator Access
	Inactive/Active User Account
	Emergency Access* (for non-clinical staff only)
	Locked/Unlocked User Account

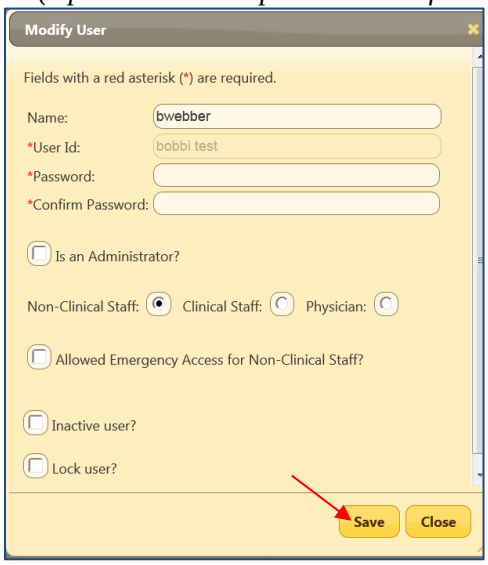
Modifying an Existing User

You are also able to modify an existing user account within the User's record:

1. Select the underlined name of the user to be modified.



2. Make any changes, as needed. *(Options will be explained in the following section of this Guide)*



3. Click the **Save** button.

Inactivating a User Account

User accounts cannot be deleted; however, accounts may be inactivated.

a. Select the **Inactivate user?** checkbox
b. Click the **Save** button

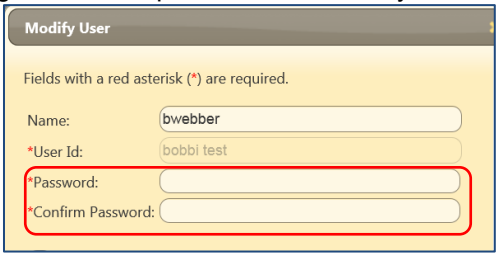
Unlocking a User Account

A Command Center account may become locked if a user attempts to log in with an incorrect password more times than is permitted. To unlock a user account:

a. Remove the check from the **Lock user?** checkbox
b. Click the **Save** button

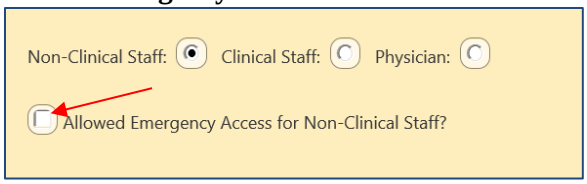
Resetting a Password

Note: You may also reset/change the user's password here if they can't remember it:

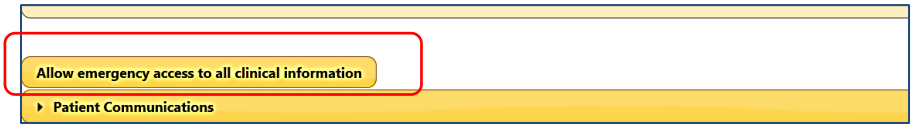


Allowing Emergency Access for Non-Clinical Staff:

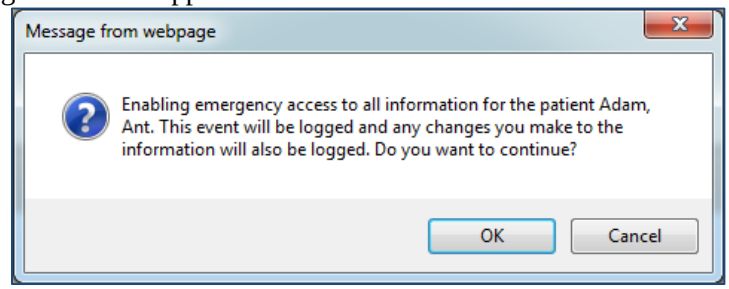
Non-Clinical Staff user accounts, by default, are unable to access Personal/Protected Health Information (PHI) in the **Command Center**. In the event of an emergency, the administrator may grant PHI access to the user by turning on the **Allowed Emergency Access for Non-Clinical Staff setting**.



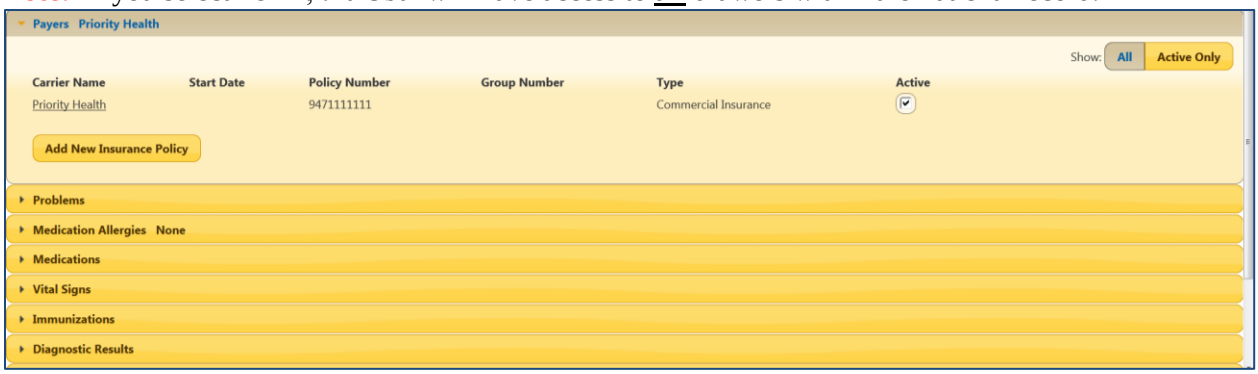
When the Non-Clinical Staff opens the Patient Record, the following option will appear under the **Payers** drawer:



The following warning screen will appear:



Note: If you select "OK", the User will have access to **all** drawers within the Patient Record.



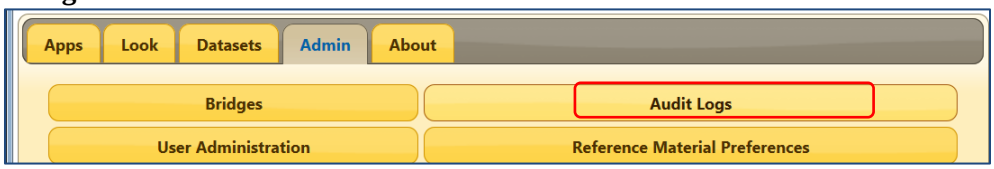
Note: Although a Clinical Staff or Non-Clinical Staff, with emergency access, has access to all drawers, it is strongly recommended that **only** the first 3 drawers are used when creating a Patient Record:

- **Personal Information**
- **Supporting Parties**
- **Payers**

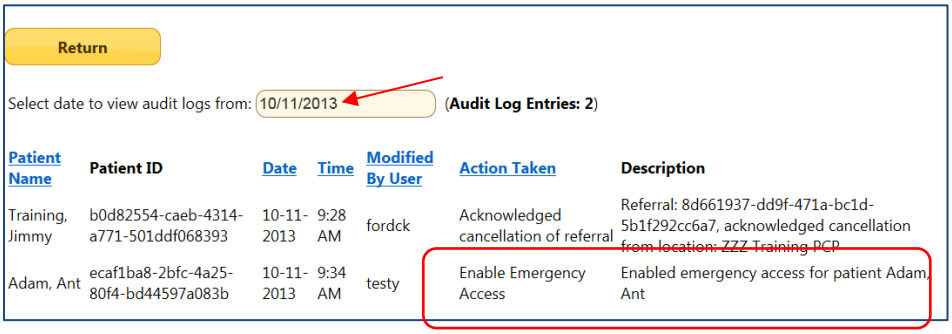
IMPORTANT: Using other drawers provides a risk of inadvertently sending clinical information without patient consent including Behavioral Health and Substance Abuse info. Therefore, remind staff to only use the first 3 drawers.

Auditing Emergency Access:

For auditing purposes, that user's access is logged. The audit trail is available within the **Admin** tab under **Audit Logs**



Enter the date in question to view the audit log. Please note that only one date at a time may be selected. There is no date range available.



Note: In most circumstances, Emergency Access is revoked upon resolution of the needed access.