Portal Account Manager

Guidance for Carolina Complete Health and Trillium Physical Health Secure Provider Portals

Portal Account Manager

- A Portal Account Manager is a role assigned to a primary contact within a provider organization
- The Account Manager is responsible for the day-to-day support of all Secure Provider Portal user accounts that are registered under the same TIN
- Email your assigned Provider Engagement Administrator or ProviderEngagement@cch-network.com to establish the first account manager for your TIN

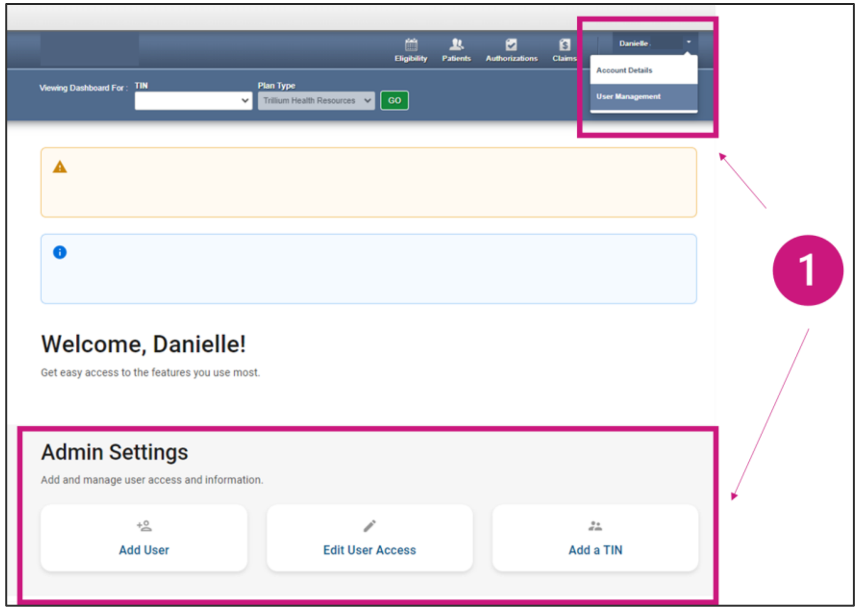
What is an Account Manager?

- Account Manager is a role within the Secure Portal that is assigned to the **primary contact within your practice. This is chosen at the discretion of the organization.**
- The purpose of this role is to help us maintain the safety and integrity of patient data.
- The Account Manager is responsible for day-to-day support of all Secure Portal user accounts that are registered under the same Tax Identification Number (TIN). These responsibilities include:
  - Approving access for new Secure Portal users
  - Assigning permissions for users based on their job responsibilities
  - Regularly adjusting the permissions of users whose roles may have changed
- Terminating users who no longer work at the practice

Accessing Account Manager Tasks

1) Click the User Management dropdown in the upper right-hand corner or use Admin Settings from the home screen to complete Account Manager actions.
2) Search for a specific user by entering their name and email address, or view a list of all users in your practice.
3) For new user accounts that need to be verified, select the Verification Pending box, click the Verify Account button, and follow instructions on the back page.

4) To view and edit details of existing accounts, click the Update User button and follow instructions on the back page

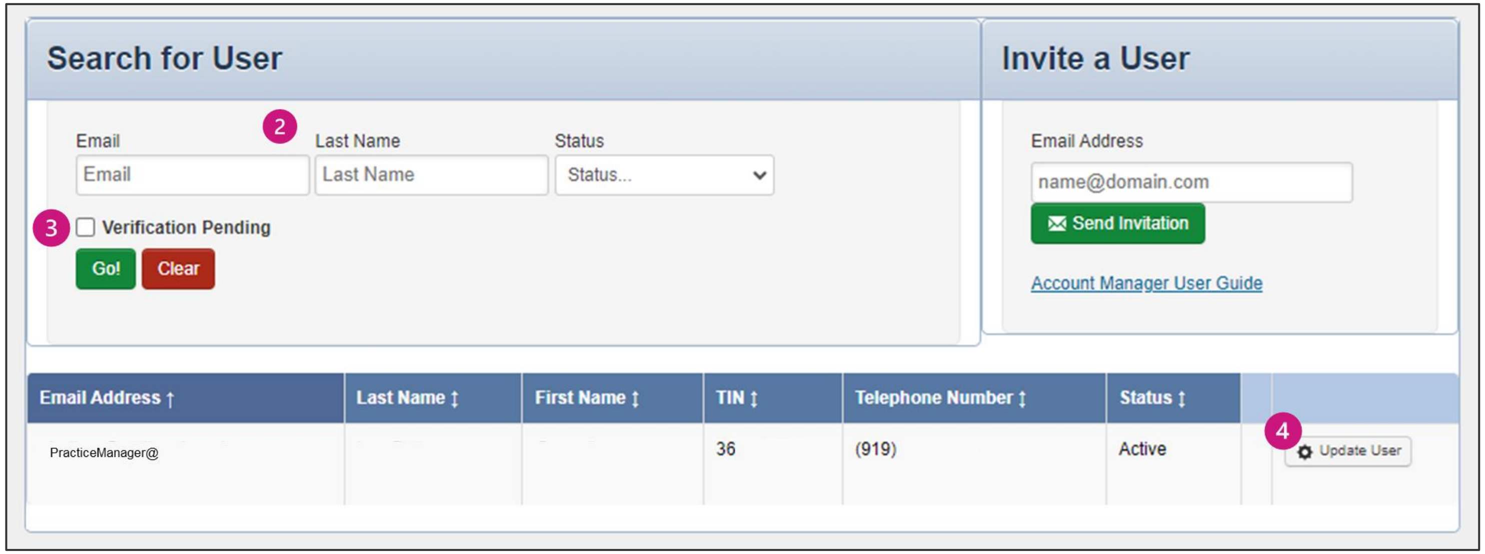


Welcome, Danielle!

Get easy access to the features you use most.

Admin Settings

Add and manage user access and information.



Email Address ↑	Last Name ↕	First Name ↕	TIN ↕	Telephone Number ↕	Status ↕	
PracticeManager@			36	(919)	Active	Update User

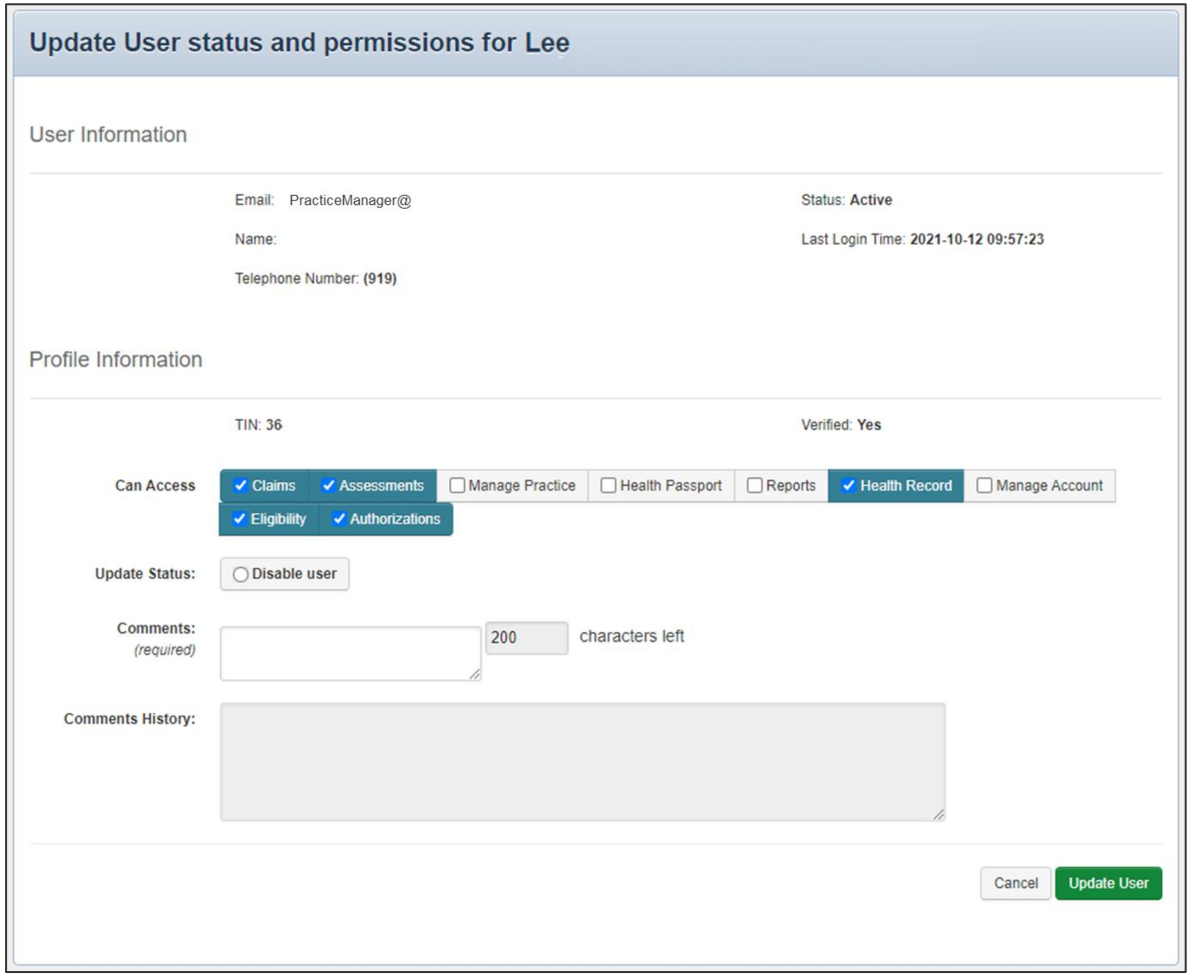
Account Manager Tasks

1. **Enabling and Disabling Users**

- Account Managers will receive an email when a user from their practice creates a new user account. The Account Manager will click Enable User to grant access to the user.
- If a user leaves the practice or no longer needs access to the Secure Portal information for that specific TIN, the Account Manager will click Disable User.

2. **Selecting/modifying access levels for users**

- Account Managers are responsible for selecting and managing the appropriate access for each user in their practice.
- Access levels include:
  - Health Records: View a patient's health records for number and type of visits, medications, Immunizations and labs, care gaps, etc.
  - Claims: View and submit claims.
  - Manage Account: Enable, disable, modify permissions for a specific TIN, and invite users to set up an account.
  - Eligibility: View and check eligibility for a specific patient.
  - Assessments: Complete or view a Health Risk Assessment (HRA) or Notification of Pregnancy (NOP) for a patient.
  - Authorizations: View and submit authorizations.



Update User status and permissions for Lee

User Information

Email: PracticeManager@

Name:

Telephone Number: (919)

Status: Active

Last Login Time: 2021-10-12 09:57:23

Profile Information

TIN: 36

Verified: Yes

Can Access: ☑ Claims ☑ Assessments □ Manage Practice □ Health Passport □ Reports ☑ Health Record □ Manage Account ☑ Eligibility ☑ Authorizations

Update Status: ○ Disable user

Comments: *(required)* 200 characters left

Comments History:

Portal Account Manager Tips

- Each TIN should have at least two Account Managers
  - For large organizations, it is recommended to have at least two Account Managers per department.
  - There is no limit on the number of Account Managers allowed under a TIN
- Account Managers should *regularly* log into the portal to:
  - Verify new portal registrations
  - Send password reset email to users whose portal account is locked due to inactivity
  - Disable / Enable a user's portal access
  - Modify portal permissions based on the user's role within your organization
- Account Managers **cannot** manage their own portal account

Tip: Always disable portal users, who no longer need portal access, especially when they leave your company.