

PerformCARE[®]

**CYBER Release 1.17:
Instructional Guide to Role-
Based Security for Adolescent
Housing Hub Security
Administrators**

Role-Based Security – Instructions for Use for Security Administrators

Table of Contents

I. Introduction 2

II. Accessing Security Administration 3

III. System Functions Screen – Search Criteria for Managing Access..... 5

IV. Searching for a User 6

V. User’s Security Access Screen..... 7

VI. Deactivating a User 11

VII. Reactivating a User 12

VIII. Editing the Provider Information File (PIF) 13

I. Introduction

Role-Based Security is CYBER functionality which allows the Security Administrators for the Adolescent Housing Hub provider agencies, as well as all other agencies that utilize CYBER, to administer their user's accounts without the assistance of the CYBER Service Desk.

Security Administrators will have access to a search function within the system which allows them to locate a specific user's CYBER account; this allows the Administrator to add or edit the user's access level to the program's records, as well as reset the user's password or unlock the user's account. Security Administrators will also have the ability to deactivate and reactivate a user's ID, as well as add new users to the system.

As Security Administrators for Adolescent Housing provider agencies, these users will also have the ability to edit the agency's contact information in their Provider Information File (PIF). This area includes the contact information for the program's Admissions Contact, which must be kept up to date; this contact information is given out by the CSA to youth seeking housing.

II. Accessing Security Administration

Users must first log-into CYBER with their User ID and Password. The log-in screen can be found via the PerformCare website – www.performcarenj.org.

The screenshot shows the top portion of the PerformCare website. The header includes the logo "NJ Children's System of Care" and navigation links: Home, Youth & Family Guide, Careers, Contact, and a search bar. Below the header is a blue navigation bar with tabs for Families, Youth, Providers, About, and CYBER. A red circle highlights the "Launch Cyber" link in the "CYBER" tab, which includes contact information for technical assistance. Below this is a "Help for Youth" section with a photo of a young girl.

The screenshot shows the "CYBER LOGIN" page. It features a form with two input fields: "Enter Login Name Here" and "Enter Password Here", followed by a "Login" button. Below the form is a consent statement regarding Protected Health Information (PHI) and HIPAA. An arrow points from the "Launch Cyber" link in the previous screenshot to the "Enter Login Name Here" field.

CYBER LOGIN

Enter Login Name Here

Enter Password Here

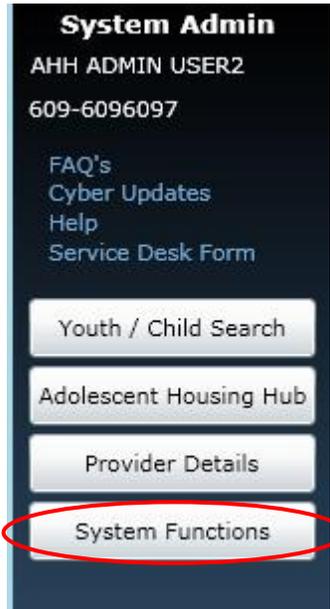
Login

As a CYBER User I understand that my work will involve access to Protected Health Information (PHI) as defined by HIPAA (The Health Insurance Portability and Accountability Act) for the purpose of providing or arranging treatment, payment or other health care operations. I also acknowledge that I am engaged by a covered entity. I further acknowledge my responsibility to protect the privacy of and to guard against inappropriate use or disclosure this PHI by logging in as a CYBER User.

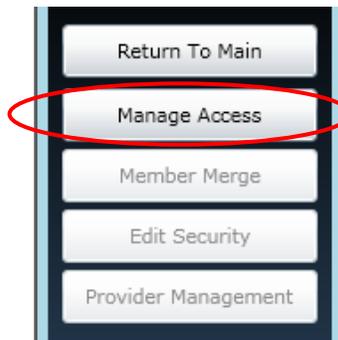
This is in compliance with "The Health Insurance Portability and Accountability Act (HIPAA) of 1996 and its implementation regulations. For more information on HIPAA please go to <http://www.hhs.gov/ocr/hipaa/> "

PerformCARE®

Security Administrators will access the Security Management area of CYBER by clicking on the System Functions button, which is located on the left-side of the user's Welcome Page.



Clicking the Manage Access button in the top left-hand corner of the window will bring the Security Administrator to the Administration screen. (*Other users will be brought to their own Edit window, where they can change their own password.)



III. System Functions Screen – Search Criteria for Managing Access

The screenshot shows the 'System Functions' interface. On the left is a dark sidebar with buttons: 'Return To Main', 'Manage Access', 'Member Merge', 'Edit Security', and 'Provider Management'. The main area has a blue header with 'System Functions' and a 'Logout' button. Below the header is the 'Search Criteria' section with the following fields:

- Program By Name: dropdown menu (All)
- Program By Trk Elem: dropdown menu (All)
- Security Groups(s): dropdown menu (All)
- Status: dropdown menu (All)
- First Name: text input field
- Last Name: text input field
- User Id: text input field

Buttons include 'Add New User Id', 'Search', 'Clear Search', and 'Print'. Below the search criteria is a table with the following columns: Login Name, First Name, Last Name, Email, Phone, Security Group(s), Programs.

The Search Criteria fields are as follows;

- Program By Name: A list of the programs in CYBER that the Security Administrator has access to; All is the default. (Most Administrators will have only one program listed here.)
- Program By Trk Elem: A list of the Tracking Element names for the programs in CYBER that the Security Administrator has access to; All is the default.
- Security Group(s): A list of the security groups that are available for the program(s) the Security Administrator has access to; the security groups are associated with user log-in types, as well as agency type. All is the default.
 - There are two user log-in types available to AHH users – AHHCM (which is a standard user) and AHHADM (which is the type given to Security Administrators)
- Status: Security Administrators can choose to search for only Active or Inactive users; All is the default.
- First Name: First Name of the user the Security Administrator is searching for; system will accept partial entries.
- Last Name: Last Name of the user the Security Administrator is searching for; system will accept partial entries.
- User ID: User ID of the user the Security Administrator is searching for; system will accept partial entries.

The buttons that are available for use are as follows;

- Add New User ID: Allows Security Administrator to add a new user to any of the programs they are open to.
- Search: Runs a search of the system based upon the Search Criteria entered.
- Clear Search: Clears all Search Criteria fields and puts them back at the default settings.
- Print: Allows Security Administrator to print the information that populates the grid once the search is complete.

IV. Searching for a User

When a Security Administrator needs to find a specific user, entering criteria into the Search fields will narrow the search results; users can leave the fields at their default settings and run a search, keeping in mind that the system will return all users that are associated with all of the programs that the Administrator has access to within CYBER, regardless of status (Active/Inactive).

Once the Administrator has completed the Search Criteria and has clicked the “Search” button, the grid below the search area will populate with the search results.

First Name Last Name

User ID

Login Name	First Name	Last Name	Email	Phone	Security Group(s)	Programs
AHHADM	Michele	Olivieri	test@performcare.org	609-689-5400	LEVEL3, AHHCM, AHHADM	OAS,Bergen County Community Action
AHHCMUSER1	AHH CM	USER1	test@test.com	609-6096101	AHHCM, LEVEL1	Bergen County Community Action Prog
AHHCMUSER2	AHH CM	USER2	test@test.com	609-6096102	AHHCM, LEVEL3	Robin's Nest - Life Link Home ,Bergen
AHHCMUSER3	AHH CM	USER3	test@test.com	609-6096103	AHHCM, LEVEL1	Bergen County Community Action Prog
AHHCMUSER4	AHH CM	USER4	test@test.com	609-6096104	AHHCM, LEVEL1	Bergen County Community Action Prog

Administrators can access the user’s security screen by double-clicking on a record in the grid.

If the Administrator chooses to print the list of users that has populated the grid, clicking on the “Print” button will create the report. The report will appear in the View Report window, and will be exportable to a PDF file, Excel, Rich Text Format, and a TIFF File.

View Report **Back to Manage Access Main Page**

1 of 2 100% Find | Next Select a format Export

Cyber Report - Manage Access

NJ Children's Care
Administered by PerformCare Behavioral Health
Mercy Company

USERID	FIRSTNAME	LASTNAME	EMAIL	Security Groups	Programs
--------	-----------	----------	-------	-----------------	----------

Select a format
Acrobat (PDF) file
Excel
TIFF file
Word

To return to the grid, the Administrator will click on the “Back to Manage Access Main Page” tab that is above the report window.

V. User's Security Access Screen

When the Administrator double-clicks on a record in the grid, the user's security access screen will open. This screen is separated into three distinct areas – Demographic/log-in information, program information, and security access information.

Deactivate

Deactivation Date <M/d/yyyy>

First, Last Name

User ID

Credentials

Password

Resets to Change_Me123

Login Attempts

Email

Phone

Assign Program(s)

Program Name	Start Date	End Date	Tracking Element	Medicaid #
OAS	2012/03/01	2012/03/01	OAS	
Bergen County Community Action Program	2012/03/01		65281512	

Assign Group(s)

Security Group	Group Description
LEVEL3	
AHHCM	Adolescent Housing Hub Care Manager
AHHADM	Adolescent Housing Hub Administrator

Available Group(s)

Security Group	Group Description
AHHCM	Adolescent Housing Hub Care Manager

PerformCARE®

At the top of the screen, the Administrator will find the basic log-in information for the user. (This information will automatically populate for an existing user, but will be blank if the Administrator is adding a new user.)

Deactivate	<input type="checkbox"/>	Deactivation Date	<M/d/yyyy>	15
First, Last Name	Michele	Olivieri		
User ID		Credentials	Training	
Password	●●●●●●	Reset Password to Default	Resets to Change_Me123	
Login Attempts	0	Reset Login Attempts		
Email	test@performcare.org			
Phone	609-689-5400			

The fields and associated buttons are defined as follows;

- Deactivate: If the Administrator needs to deactivate a user, they must first check-off this box.
- Deactivation Date: This field will automatically populate with today's date once the Deactivate check-box is selected; the date can be changed to a future date but cannot be changed to a date in the past.
 - Please refer to page **12** for more information on deactivating a user.
- First, Last Name: First and Last Name of the user (can be edited at any time).
- User ID: Will be automatically populated for an existing user and cannot be edited; this field will be blank and open to editing prior to saving the record if entering a new user.
- Credentials: The credentials of this user (LCSW, LSW, etc.); will be used in the future to automatically populate other areas of the system. (This field is optional.)
- Password: Will be automatically populated and masked for an existing user and cannot be edited. This field will be blank and locked for editing if entering a new user.
 - Please note: Every 90 days, users will receive notification that they need to change their passwords. New passwords must be at least 8 characters long, with at least 3 out of the 4 following character types: upper case letters, lower case letters, numbers and/or special characters. This notification will occur when the user logs into CYBER.
 - Users can change their own passwords at any time by clicking on the "Systems Functions" button on their Welcome Page, and then the "Manage Access" button.
- Reset Password to Default: Clicking this button will reset this user's password. If there is an email address for the user in the system (see Email field), the system will immediately send the user a new temporary password (once Save or Save and Exit is clicked at the bottom of the screen). If the Email field is blank, the user's password will be reset to the default (which is listed next to the button as "Change_Me123") and the System Administrator will receive a message stating that the password has been reset. (System Administrators will need to let the user know that the password has been reset to the default; the user will not receive notification. The change will not take effect until Save or Save and Exit has been clicked.)
- Login Attempts: Lists the number of login attempts the user has had in one session before locking their account (not available for edit). The user has a maximum of 3 attempts before their account is locked.
- Reset Login Attempts: Administrators will use this button when a user has locked their account after trying to login with an incorrect password or user ID; users will receive a message on the login screen saying that their account is locked and that they must contact their System Administrator to have their account unlocked.
- Email: The user's email address (can be edited).

- Phone: The user's phone number (can be edited).

Below this area is the Assign Program grid.

Phone

Assign Program(s)

Program Name	Start Date	End Date	Tracking Element	Medicaid #
OAS	2012/03/01	2012/03/01	OAS	
Bergen County Community Action Program	2012/03/01		65281512	

The grid will be populated with any programs that this user is currently associated with. The grid will show the name of the program, the start date that the user gained access, an end date if the user is no longer associated with that program (this field will auto-populate with the date of deactivation from the top of the screen if the Administrator deactivates the user; the auto-population will not occur until the Administrator clicks the Save or Save and Exit button at the bottom of the window), the Tracking Element associated with the program and the Medicaid ID # of the program.

Clicking the "Add a Program" button will bring up a list of programs that the Administrator has access to and can assign to users.

The Program Name menu will allow the Administrator to choose a program to associate the user with; the start date (and end date) can also be entered here. If the Administrator needs to end the user's access to one program without deactivating their access to the system, an end date would be entered in this window (the end date must be either today's date or a date in the future, it cannot be back dated). If the user has been deactivated, an end date will automatically populate with the deactivation date.

Once the Administrator clicks the "Save and Exit" button, they will be brought back to the program grid and the new program will be listed there (along with any changes made to an existing program). Clicking on the Exit button will not save the changes and will return the Administrator back to the program grid.

PerformCARE®

In order to end a user's access to a program, the Administrator will double-click on the program in the grid and enter an end date in the Add/Edit Programs window. Please note that this does not deactivate the user, even if this is the only program they have access too.

Below the program grid, the Administrator will find the Security Group assignment and removal area.

Assign Group(s)	
Security Group	Group Description
LEVEL3	
AHHCM	Adolescent Housing Hub Care Manager
AHHADM	Adolescent Housing Hub Administrator

Available Group(s)	
Security Group	Group Description
AHHCM	Adolescent Housing Hub Care Manager

>> Remove Security Group

<< Add Security Group

Exit Save and Exit Save

The "Assign Group(s)" area on the left will list the security groups that are currently attached to this user's ID; if this is a new user, this area will be blank. If this is an established user, this area will include the user's security as it was set up for this release. In order to add security groups to the user's ID, the Security Administrator will go to the "Available Group(s)" area on the right, click once on a group to highlight it, and click the "Add Security Group" button in the middle of the two grids. The new group will now appear on the right, in the Assign Group(s) grid.

The Security Groups that appear in the Available Group(s) grid first, which start with the agency type (AHH), have a title associated with them (Care Manager, or Security Administrator).

The Levels that appear on the list – Level 1 and Level 3 – pertain to the security set-up; these levels dictate what functions a user has access to. Level 1 users will have access to all of the AHH-specific functionality, including the ability to admit and discharge youth; only Level 3 users will have access to reporting (please note that this functionality will not be available on the day of the release; it will become available once data is collected in the system).

If an Administrator needs to edit, or remove, a Security Group from a user's profile, they need to highlight it on the "Assign Group(s)" grid and click on the "Remove Security Group" button in the middle of the two grids. The group will be removed from the Assign Group(s) grid on the right and will appear again on the left in the Available Group(s) grid.

Clicking the "Save and Exit" or "Save" button will save any changes made.

Please note: While creating a new User ID, clicking the "Save" button will lock the User ID field from editing; the new ID will be created in the system and cannot be changed, even if the remainder of the information is not completed.

- It is recommended that the Security Administrator create ID's in the following format – "first name initial" "last name" (i.e., jsmith); a number can be added if the system finds that the ID already exists (i.e., jsmith1).

VI. Deactivating a User

When a user leaves an agency, it is recommended that the Administrator deactivates the user’s access as soon as possible so that the security and privacy of the PHI that is housed in CYBER continues to be protected.

The Administrator will first need to search for the user’s security information (see page 6). Once the correct user is located, the Administrator can then deactivate their access.

The screenshot shows a user management form with the following fields and controls:

- Deactivate:** A checkbox, currently unchecked, highlighted with a red box.
- Deactivation Date:** A date selection field with a calendar icon, currently showing '15', also highlighted with a red box.
- First, Last Name:** Two text input fields containing 'Michele' and 'Olivieri'.
- User ID:** A text input field containing a blurred ID.
- Credentials:** A text input field containing 'Training'.
- Password:** A text input field with masked characters (dots), a 'Reset Password to Default' button, and the text 'Resets to Change_Me123'.
- Login Attempts:** A text input field containing '0' and a 'Reset Login Attempts' button.
- Email:** A text input field containing 'test@performcare.org'.
- Phone:** A text input field containing '609-689-5400'.

Checking off the “Deactivate” box will prompt the system to enter the current date into the Deactivation Date field; this date can be changed to one in the future (cannot be back-dated). In order for the deactivation to take place in the system, the Administrator must click either Save or Save & Exit at the bottom of the screen.

The 'Assign Group(s)' dialog box contains the following table:

Security Group	Group Description
LEVEL3	
AHHCM	Adolescent Housing Hub Care Manager
AHHADM	Adolescent Housing Hub Administrator

At the bottom of the dialog, there are three buttons: 'Exit', 'Save and Exit', and 'Save'. The 'Save and Exit' button is highlighted with a red box.

If the deactivated user currently has work assigned to them that is in progress or in draft form, the Administrator will receive a notification message (via pop-up box) that there is outstanding work attached to this deactivated ID as soon as the Deactivate box is checked off.

If the Administrator receives this message, they may see the user’s draft progress notes listed on their Welcome Page under the Deactivated Users/In Progress grid.

VII. Reactivating a User

Administrators may need to reactivate a user's ID if that user is now associated again with the agency.

In order to reactivate a user, the Administrator must first search for the user in CYBER. By entering information into the search criteria on the Manage Access window (Program Name, Tracking Element, First Name, Last Name, etc), and then selecting "Inactive" in the Status pull-down menu will create a search of only those users that are inactive that fit the search parameters.

Search Criteria

Program By Name	<input type="text" value="All"/>			
Program By Trk Elem	<input type="text" value="All"/>			
Security Groups(s)	<input type="text" value="AHHCM"/>		Status	<input type="text" value="All"/>
First Name	<input type="text"/>		Last Name	<input type="text"/>
User ID	<input type="text"/>	<input type="button" value="Search"/>	<input type="button" value="Clear Search"/>	<input type="button" value="Add New User ID"/>
			<input type="button" value="Print"/>	

Once the user's information appears in the grid, the Administrator can open their details by double-clicking on the record.

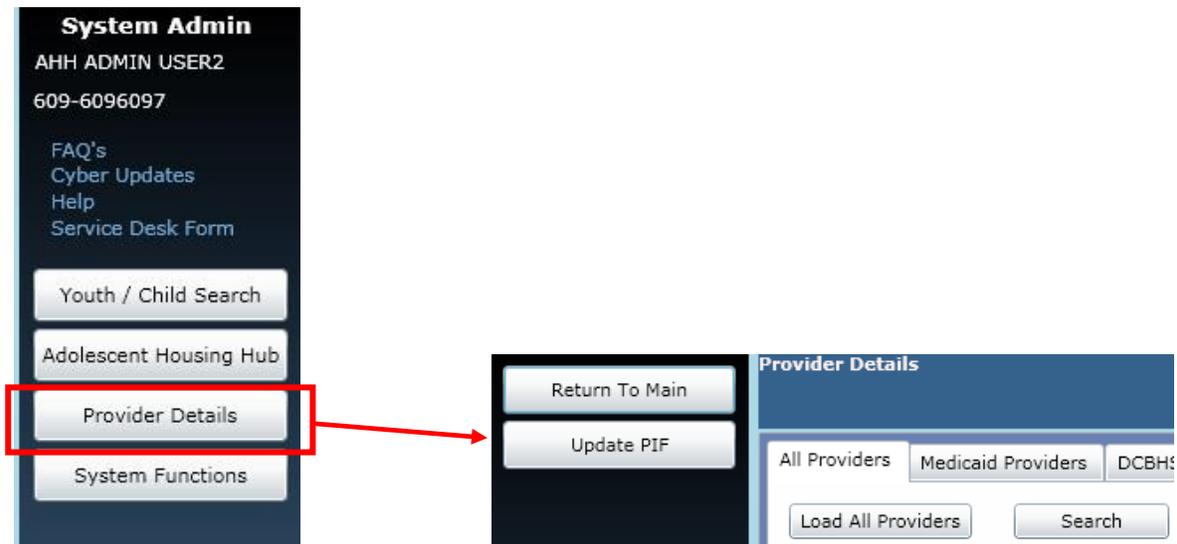
At the top of the User ID Details window, the Deactivate check-box will be selected; removing the check from the box will remove the Deactivate Date. The System Administrator should then go through the rest of the User ID Details window, associating the appropriate programs and making sure that the Security Group(s) is correct. Once completed, clicking Save or Save and Exit will save the changes and reactivate the user's ID.

- Please note – the programs that the user was associated with will not be available to be re-opened; the Administrator will need to add the programs again to the user's profile. Also, the user's password will still be in the system as it was when the user was deactivated. The Administrator may need to reset the user's password if they don't recall it.

VIII. Editing the Provider Information File (PIF)

Security Administrators for adolescent housing providers have the ability to edit the contact information for their agency in CYBER via the Provider Information File (PIF). This area of CYBER also houses information regarding who the program can service; this area can only be edited by OAS staff.

To reach the PIF screen, Security Administrators will first click on the Provider Details button on their Welcome Page. This will bring them to Provider Details, where they will have an active Update PIF button. Clicking here will bring the Administrator to the PIF screen.



Location
 Bergen County Community Action Program

Site/Program
 Bergen County Community Action Program

Mailing Address City State Zip code
 3959 BROADWAY TRENTON NJ 08691

Admissions Contact Phone Contact Email Contact
 Chip Annadale 1-609-5551212

Capacity
 25

Age Specifiers

<input checked="" type="checkbox"/>	AGE 16
<input checked="" type="checkbox"/>	AGE 17
<input type="checkbox"/>	AGE 18
<input checked="" type="checkbox"/>	AGE 19
<input type="checkbox"/>	AGE 20
<input type="checkbox"/>	AGE 21

Specifiers

<input checked="" type="checkbox"/>	Adjudicated/No Tier	Y
<input checked="" type="checkbox"/>	Homeless Youth	Y
<input type="checkbox"/>	Mental Health Diagnoses	N
<input type="checkbox"/>	Open DYFS Case	O
<input type="checkbox"/>	Parent with Child	Y
<input type="checkbox"/>	Pregnant	N
<input type="checkbox"/>	Tier I	Y
<input type="checkbox"/>	Tier II	N
<input type="checkbox"/>	Tier III	N

Gender Served

Male
 Female

Site Type

PSH
 STLP
 TLP

Cancel Submit

Before being able to edit any fields, the Administrator must first select a Location from the pull-down menu at the top of the screen; doing so will populate the rest of the fields.

*Please note – the only fields that can be edited by a Security Administrator are the Site/Program Name, Mailing Address, and Admissions Contact fields. All others (that are grayed out in the example above) can only be edited by the OAS; if changes need to be made, someone from the provider agency must contact OAS directly.