CYBER Password Reset Functionality
Presented by the PerformCare Training Unit

August 2019 – (01362)
Objectives

The objective of this training is to provide an overview of CYBER Password Reset Functionality for all Providers. We will cover:

- Accessing and Logging into CYBER
- Edit a User Profile
- Login Scenarios and their Solutions
- Username States
- Reset a Password
- The Temporary Password
- Who to Call for Assistance
- Resources
Helping Families Across New Jersey
1-877-652-7624

- Behavioral Health
- Intellectual/Developmental Disability Services
- Substance Use Treatment

Launch CYBER
Children's System of Care Providers can access the CYBER system here.

For Providers
For guidance, resources, training materials, and additional support.

Family Resources
Find community resources and supports tailored to your family's specific needs.

Help for Youth
If you are between the ages of 5 and 21 and need help, Meet Me at the Table is here.

The Latest
March 25, 2019: Join PerformCare on April 4 for a special event featuring the documentary, Autism in Love.
Providers

Find details, updates, clinical criteria, and other resources of use for all providers.

- Register for training or access archived training.
- Get forms, including the Clinical Summary Template and consent forms for Substance Use treatment.
- Find resources you need and get answers to our frequently asked questions (FAQs).
- DCP&P staff — get information about accessing services through PerformCare.
- See a list of out-of-home (OOH) providers in the New Jersey Children's System of Care provider directory.
- Information about CSOC Summer Camp Services for Providers.

Service Desk and CYBER technical support for providers

Phone:
1-877-652-7624

Online:

Complete this online Customer Service Request Form to address CYBER technical issues, and questions regarding clinical, billing, eligibility, and reporting issues. You will need your Provider Agency ID available to submit a request.
Provider Training

Providers can utilize the documents and modules below for CYBER and Children’s System of Care (CSOC) provider operations training to better support the quality care of New Jersey's families and youth.

Are you looking for certification training for behavioral assistants and Information Management Decision Support (IMDS) tools or ongoing trainings on CSOC topics relevant to you or your staff? CSOC partners with Rutgers University to provide these trainings and more to CSOC providers and other community members.

- Adolescent Housing Hub (AHH)
- Annex A Addendum
- Assessments
- Billing and Claims
- Care Management Organization (CMO)
- Child and Adolescent Needs and Strengths (CANS)
- Division of Child Protection & Permanency (DCPP)
- Family Support Organizations (FSO)
- Family Support Services (FSS)
- General Trainings for All CSOC Providers
- Intensive In-Community (IIC)/Behavioral Assistance (BA)/Social Emotional Learning (SEL)
- Intensive In-Home (IIH)/Individual Support Services (ISS)
- Mobile Response & Stabilization Services (MRSS)
- Multisystemic Therapy (MST), Family Functional Therapy (FFT), Partial Hospitalization Program (PHP), Children’s Out Of Home (OOH)
- Reports
- Security
Provider Training

Providers can utilize the documents and modules below for CYBER and Children’s System of Care (CSOC) provider operations training to better support the quality care of New Jersey's families and youth.

Are you looking for certification training for behavioral assistants and Information Management Decision Support (IMDS) tools or ongoing trainings on CSOC topics relevant to you or your staff? CSOC partners with Rutgers University to provide these trainings and more to CSOC providers and other community members.

- Adolescent Housing Hub (AHH)
- Annex A Addendum
- Assessments

Security

View sessions and documents

- Family Support Services (FSS)
- General Trainings for All CSOC Providers
- Intensive In-Community (IIC)/Behavioral Assistance (BA)/Social Emotional Learning (SEL)
- Intensive In-Home (IIH)/Individual Support Services (ISS)
- Mobile Response & Stabilization Services (MRSS)
- Multisystemic Therapy (MST), Family Functional Therapy (FFT), Partial Hospitalization Program (PHP), Children's Out Of Home (OOh)
- Reports
- Security
Provider Training

Providers can utilize the documents and modules below for CYBER and Children’s System of Care (CSOC) provider operations training to better support the quality care of New Jersey’s families and youth.

Are you looking for certification training for behavioral assistants and Information Management Decision Support (IMDS) tools or ongoing trainings on CSOC topics relevant to you or your staff? CSOC partners with Rutgers University to provide these trainings and more to CSOC providers and other community members.

- Adolescent Housing Hub (AHH)
- Annex A Addendum
- Assessments

Security

View sessions and documents

- Adolescent Housing Hub Role Based Security 20120423 (PDF)
- CME Instructional Guide to Role Based Security 20120228 (PDF)
- CYBER Security Administrator Instructional Guide 20180914 (PDF)
- CYBER Security Administrator Quick Reference Guide 20180507 (PDF)
- MRSS Instructional Guide to Role Based Security 20120228 (PDF)
- MST-PHP Instructional Guide to Role Based Security 20120228 (PDF)
- OOH Instructional Guide to Role Based Security 20120228 (PDF)
- Password Reset for All Providers 20190219 (PDF)
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 of 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/

CYBER contains substance abuse diagnosis and treatment information that is protected by federal confidentiality rules (42 CFR Part 2). CYBER users are not permitted access to that information without a valid written consent that meets the requirements of 42 CFR Part 2. Users that access such confidential information pursuant to a valid written consent are prohibited from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.

Please CLEAR your browser Cache before using this new version of CYBER

Username

Password

Password

LOGIN

Customer Service Request Form  |  Forgot Password?
Editing the User Profile

• The CYBER Username is accessed using the System Functions button on the left-side of the Welcome Page.

• Users can edit only three fields in their CYBER user profile: Password, Email and Phone.

• To access the user profile, click on the System Functions and then Manage Access buttons on the upper left-side of the screen.
It is required that users enter their current email address and work phone number into the Email and Phone fields.

Entering a valid Email allows the system to send a temporary password to the user.

- Users can access the CYBER password reset screen and change their password.
- Users can reset their password at any time, without contacting the Security Administrator or the Service Desk.

**Note:** A valid email address contains the correct email address including the '@' symbol and no extra spaces at the start, or end of the email.

Users may also update their password once logged into CYBER by clearing the encrypted password (dots) and typing a new secure password. The user must then click **Save Login Info** to save the changes.
Security Administrators can change their own passwords from inside CYBER following these steps:

1. Enter your name or User ID and click Search.
2. When the name appears double click and the User Login Details will open.
3. Clear the encrypted password (dots) and enter a new secure password.
4. Click Save and Exit.
5. Log out of CYBER and back in.
6. Contact PerformCare for assistance.
Each time a user logs into CYBER, the system checks that the Username is valid and active and the associated Password matches the password in the user’s profile.

**IMPORTANT NOTE:** Each attempt is counted and is cumulative. For example, the user may have tried to log in four times last week unsuccessfully (system counts 4 attempts) and then tries again today (system counts 5 attempts and is locked). The user will receive the password reset option.

There are other login issues that can arise if the user enters incorrect information or if the Username that is entered is no longer active.

The next series of slides will go through each scenario.
Valid Username and Incorrect Password = Locked

**Scenario:** User attempts to log in with an active Username and incorrect Password. The system will display the message:

"The Username or the Password combination entered does not match our records. Please check and try again."

User attempts to log in 5 consecutive times unsuccessfully, they will receive the following screen:

**Solution:** User should enter an email address associated with the Username. **Note:** Some users have more than one CYBER Username. Users may associate the same email address to any CYBER Username.
Scenario: User entered a Username that is not valid (does not exist in CYBER) – users will receive the following message under the Login button:

After the 5th attempt, the user will see a blank screen and the following message:

You have attempted to login too many times. Please close your browser and try again. If you are still unable to login, please contact your Security Administrator.

Solution: Check the Username, close all open Internet windows and try again. This action is called ‘Refreshing the browser.’
After entering an email and clicking the ‘RESET PASSWORD’ button, the system validates that the information entered matches what is in the user’s profile.

If the combination entered matches the system, the user will be emailed a temporary, random password.

The user should click the EXIT button.

Users are given 5 attempts at resetting their password using their Username and Email combination.
Invalid, Incorrect or Missing Email = Deactivated

Scenario: Each time the user attempts to reset the password using the Reset Password screen, and the Username and Email combination entered does not match what is in the user’s profile, the user will receive the following message – ‘The email address entered does not match our records. Please check and try again. Your account will be deactivated after (number) more unsuccessful attempts.’

After the user enters an incorrect email address for the 5th time, the system will deactivate the account and a new message will display, ‘Your account is deactivated because of too many failed login attempts. Please contact your Security Administrator.’
Invalid, Incorrect or Missing Email (Cont’d)

If the User deactivates their account, they will receive a message indicating that they need to contact either their Security Administrator for assistance as shown in the example below:

Solution: Once this message appears, the user must contact their Security Administrator to access CYBER. The Service Desk cannot assist the user in this case.

If the user is successful at entering the correctly associated email before 5 attempts, the temporary password is sent immediately. If you do not receive an email with the temporary random password:

- Confirm that your Email is working and you can receive email
- Confirm the Email Address on your User Profile with your Security Administrator
Forgot Password Feature

The ‘Forgot Password?’ link - This feature may be used when or if the user cannot remember their password.

Clicking the ‘Forgot Password?’ link prompts the user to enter their Username and click OK.
There are 3 ‘states’ a Username may be in:

- Valid and active
- Invalid
- Not active; deactivated

1. The Username is **valid** and **active** when the user clicks OK, the user will see ‘Enter the email address associated with the Username and we will send you a temporary password. If you do not have your email address or if your email address does not match please contact your security administrator.’

2. The Username is **invalid**, user will see ‘Username entered above does not match our records.’ Click cancel and try again.
Username States (Cont’d)

3. Username is **not currently active; deactivated**, the user will see, ‘Your Username is not currently active. Please contact your Security Administrator.’

Contact your Security Administrator.

```
Forgot Password
Username
OK  Cancel
Your Username is not currently active. Please contact your Security Administrator.
```
Use Strong Passwords

Strong passwords are required to access CYBER. A strong password will have at least 8 characters including at least three of these four types of characters:

1. uppercase letter (A B C)
2. lowercase letter (d e f)
3. numeric character (numeric: 2 4 9)
4. non-alphanumeric character (non-alphanumeric: # $ % & - _)

Examples of weak password Choices:

- dates, date of birth
- children’s/pet’s names
- proper nouns/names

Note: The system will remember and not permit reuse of your last four passwords.
The Temporary Password

The temporary random password will appear in your email:

- The temporary password can be copied from the email message and pasted or typed into the CYBER login screen.
- Once the user logs in successfully with the temporary password, they will be asked to select a new password.
- The temporary password cannot be used again once the password is reset.
The Temporary Password Cont’d

A message will appear when the password has been changed successfully.

If your browser saves your password and you reset the password, you may need to change the saved password.

**90 Day Password Requirement**
You must change your password every 90 days. If it has been 90 days since your last password change, when you attempt to log in, CYBER will display the Password Reset Window and require you to identify yourself and reset your password.
Reminder Notification

- CYBER will keep track of the last password change and will display a **reminder notification** when the password needs to be changed, 5 days prior to the 90 day limit.

- 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.

- The system will remember and not permit reuse of users’ last four passwords.

- **Note:** The reminder notification will occur when the user logs into CYBER.
90 and 180 Day Rules for User Lockout/Deactivation

• You may lock or deactivate your own username if you do not log into CYBER regularly.

• If you do not log into CYBER for 90 consecutive days, your username will be automatically locked and you will be forced to reset your password to log back in. When you attempt to log in after 90 days, you will receive the message, ‘Your account has been locked because you have not logged into CYBER in the past 90 days. Please click OK to reset your password.’ You can click the ‘Forgot Password?’ link from the CYBER login page to access the Reset Password feature.

• If you do not log into CYBER for 180 consecutive days, your username will be automatically deactivated.
  • When you attempt to log in after 180 days, you will receive the message, ‘Your Username is not currently active. Please contact your security administrator.’
  • You should contact your agency’s Security Administrator(s) to reactivate your account.
  • The Service Desk will not be permitted to reactivate your account and will refer you to your security administrator.
Who to Call for Assistance

• If you have closed your browser windows and then attempted to reset your Username and Password and have been unsuccessful, always contact your Security Administrator for assistance *first*.
Resources

- PerformCare Website [www.performcarenj.org](http://www.performcarenj.org)
- CYBER > Access requirements: [http://www.performcarenj.org/cyber/access-requirements.aspx](http://www.performcarenj.org/cyber/access-requirements.aspx)
- PerformCare website Training web page [http://www.performcarenj.org/provider/training.aspx#security](http://www.performcarenj.org/provider/training.aspx#security)

PerformCare Customer Service
[www.performcarenj.org/ServiceDesk](http://www.performcarenj.org/ServiceDesk)
1-877-652-7624
Care is the heart of our work.