

Security Awareness and CYBER

Guidelines for All CSOC Providers

July 2019 - #01245

PerformCARE[®]

Delivering
High-Quality
Service and Support

Understand/Recognize:

- Your obligation to protect PHI data in CYBER
- Strong password configuration
- Password reset functionality
- How to safeguard passwords
- How to lock your computer for extra protection
- How to secure your network
- Public WIFI risks
- What to do if your Network/Computer is compromised

CYBER Login

Below the CYBER login area is a statement that, as a CYBER user, you acknowledge your responsibility to protect the privacy of, and to guard against, the inappropriate use of the PHI contained within the system.

This statement will appear each time you log in.

Your CYBER password defends and protects PHI in CYBER.

CYBER 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 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

[Forgot Password?](#)

Protected Health Information or PHI should not be shared in email messages. Do not include youth PHI or potential PHI in email messages to PerformCare.

PHI consists of any health details about a youth associated with identifying information such as:

- Name or Initials of a Name
- Address
- Date of Birth
- Social Security Number
- CYBER ID
- Authorization number
- Provider Name/Medicaid number
- Dates of Service

The Service Desk Request Form allows you to send inquiries about youth to PerformCare securely: www.performcarenj.org/ServiceDesk

Never share any passwords with anyone,
not even your CYBER Security Administrator.

Use a strong, complex password.



A strong, complex password:

- Is eight or more characters in length
- Contains both uppercase and lowercase letters
- Contains at least one number
- Contains at least non-numeric (# \$ % & - _)
- Contains non-sequential number or letters
- Does not contain a password you have used in the past 4 password cycles
- Does not contain common information (birth dates, pet names, family names, dictionary words, local sport teams, etc.)

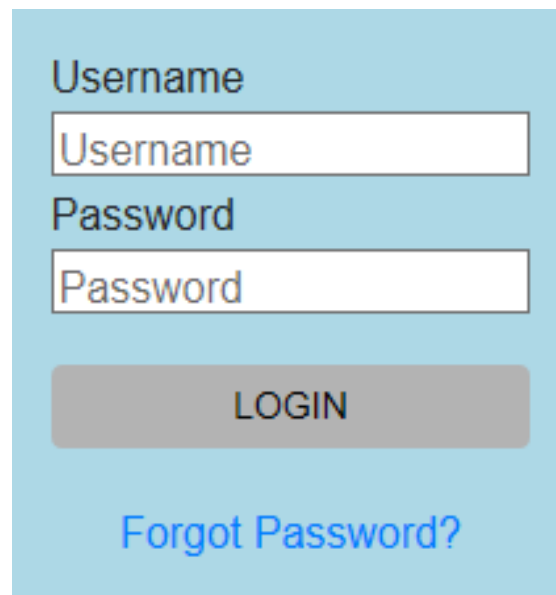
How often should your CYBER password be reset?

CYBER passwords should be reset at least every 90 days or anytime you are locked out.



If you forget your password, you can reset your password without contacting the CYBER Service Desk.

Use the CYBER Password reset functionality.



The image shows a light blue rectangular interface for password management. It contains the following elements from top to bottom: the label 'Username' above a white text input field containing the placeholder text 'Username'; the label 'Password' above another white text input field containing the placeholder text 'Password'; a grey rectangular button with the text 'LOGIN' in black; and a blue text link that says 'Forgot Password?'.

For Password Reset for All Providers, See [Additional Training References](#)

Reset Your CYBER Password

- Enter the correct Username for the account and enter your (incorrect) password three (3) times.
- CYBER will ask for your email associated to that Username.
- Enter the associated email.
- A temporary random password will be sent to the email.
- Close all browser windows.
- Copy and paste the random temporary password into the CYBER login screen.
- CYBER will display a password reset screen.

Reset Password

Username:

Enter the email address associated with the Username and we will send you a temporary password.

Email Address

RESET PASSWORD EXIT

It is extremely important to properly safeguard your password.

- **Do not write down your passwords anywhere.**
- Do not store your passwords in a document on your computer.
- **Never share your passwords with anyone.**
- All of your password must be strong passwords.

Working in a public location - Lock your computer!

If you leave your computer unattended at home or in a public place (library), it is a security risk!

The quickest way to lock your computer is to simply **click the Windows Key + L*** at the same time.



*Microsoft PC users

Public networks or WIFI Internet connections are offered at many public places such as coffeehouses, hotels, libraries, airports and other locations.

There are two concerns regarding public WIFI:



- Anyone and everyone can access a public network making your computer very unsecured.
- People may see the data on your screen.



Recommendation:

**Do not use a public network if you have secure options.
Work in a private office or use a Virtual Private Network (VPN).**

If you are usually working from home, you should ensure that your home's wireless network is secured.

If your home's wireless network is unsecured, you are putting yourself at risk against skilled hackers who may be able to hack into your devices to extract information.

**Add a complex password to your network
and change your password regularly!**

If you are aware that your agency network or computer has been compromised, **change your passwords immediately** and then report it to your Security Administrator and contact PerformCare.

**Contact PerformCare:
1-877-652-7624**

Additional References

For more information on Training or CYBER Security see these links below.

PerformCare Training webpage: <http://www.performcarenj.org/provider/training.aspx>

Security Section on Training

- <http://www.performcarenj.org/provider/training.aspx#security>

Password Reset for All Providers

- <http://www.performcarenj.org/pdf/provider/training/security/instructional-guide-password-reset-all-providers.pdf>

Quick Reference Guide to Secure Email from PerformCare

- <https://www.performcarenj.org/pdf/provider/training/security/quick-reference-guide-to-secure-email.pdf>

Care is the
heart of
our work.

PerformCARE[®]