Security Awareness and CYBER

Guidelines for All CSOC Providers

March 2025 – (02689)

PerformCare®

Delivering
High-Quality
Service and Support

Understand/Recognize:

- Protect Personal Health Information (PHI) /Personally Identifiable Information (PII)

- Security Best Practices

  - Passphrase configuration

  - CYBER Password Reset

  - Safeguarding your computer

  - Securing your network

- Public WIFI risks

- Network/Computer is compromised

- References

CYBER Login

The CYBER Login states you acknowledge your responsibility to protect the privacy of and to guard against inappropriate use or disclosure of PHI by logging in as a CYBER User.

Your CYBER passphrase defends and protects Protected Health Information (PHI) and Personally Identifiable Information (PII) 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 acknowledgement 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 use diagnosis and treatment information that is protected by federal confidentiality rules (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 person with substance use treatment needs.

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

Username

Username

Password

••••••••••

LOGIN

Customer Service Request Form | Forgot Password?

© 2024 - CyberAng 1.0.0.455.21-2.0.0.18-10

This statement will appear each time you log in.

Protect PHI/PII

- PHI/PII should not be shared in email messages unless encrypted.

- PHI/PII should never be included in the subject line of an email, even when an email is sent securely.

- Do not include youth PHI or potential PHI in email messages to PerformCare.

- PHI is any individually identifiable health information that relates to a youth's past, present, or future physical or mental health condition, health care services provided to the youth, or health care payment information.

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

PHI and PII

PHI data in CYBER can include

- CYBER ID

- Authorization number

- Medicaid number

- Dates of Service

- Progress Notes

- Treatment Plans and Assessments

PII data can include

- Name or Initials of a Name

- Address

- Date of Birth

- Social Security Number

- Location of birth, race, religion, weight, geographic indicators, employment information, education information, rental applications

- Passport, taxpayer ID, driver's license, or other government-issued ID number

- Facial recognition, fingerprint, handwriting, retinal scans, voice signature, etc.

- Credit or debit card number

Security Best Practices

- Keep your computer updated.

- Use up-to-date, Anti-virus, anti-malware software.

- Watch out for smishing (text scams), phishing scams, spyware, and malware.

- Don't open suspicious emails or links.

- Use a passphrase. It is the first line of defense against unauthorized access to your computer.

- Use a trusted secure network or a Virtual Private Network (VPN).

- Back up your data.

PerformCARE®

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

No one should ever ask you for your passphrase. If that occurs,
please report it to the PerformCare Service Desk.

Passphrase

To enhance security, PerformCare is upgrading the password requirements to passphrase requirements.

Passphrase requirements are:

- **The passphrase must be a minimum of 20 characters.**

- **Users cannot re-use their 5 previous passphrases.**

Passphrases *should* contain a combination of:

- Uppercase characters

- Lowercase characters

- Numbers

- Only these special characters: $ @ # ! () {} [] ^ & %

Passphrase Suggestions and Examples

Make your Passphrase complex. Try using some of the following ideas:

- **Random words**: The words in your passphrase may have no connection.

- **Capitalization**: Capitalize the random letters.

- **Numbers and specific characters**: 0 to 9 or specific approved characters.

- **Non-English words**: Words in a language other than English (no accented characters).

- **Misspellings**: Intentionally misspelled words.

- **Mnemonic form or Acronym**: Create your own way to make it easy to remember. (Mnemonic example: PEMDAS = Please Excuse My Dear Aunt Sally)

- **Refrain from using common phrases such as song lyrics or movie quotes**.

- PurpleElephantsSlidingOverClouds

- 3@pples&Or@nges#Ban@nas

- ChocolateCakeIsMyFavouritedess3rt

These are examples only. Please do not use these examples.
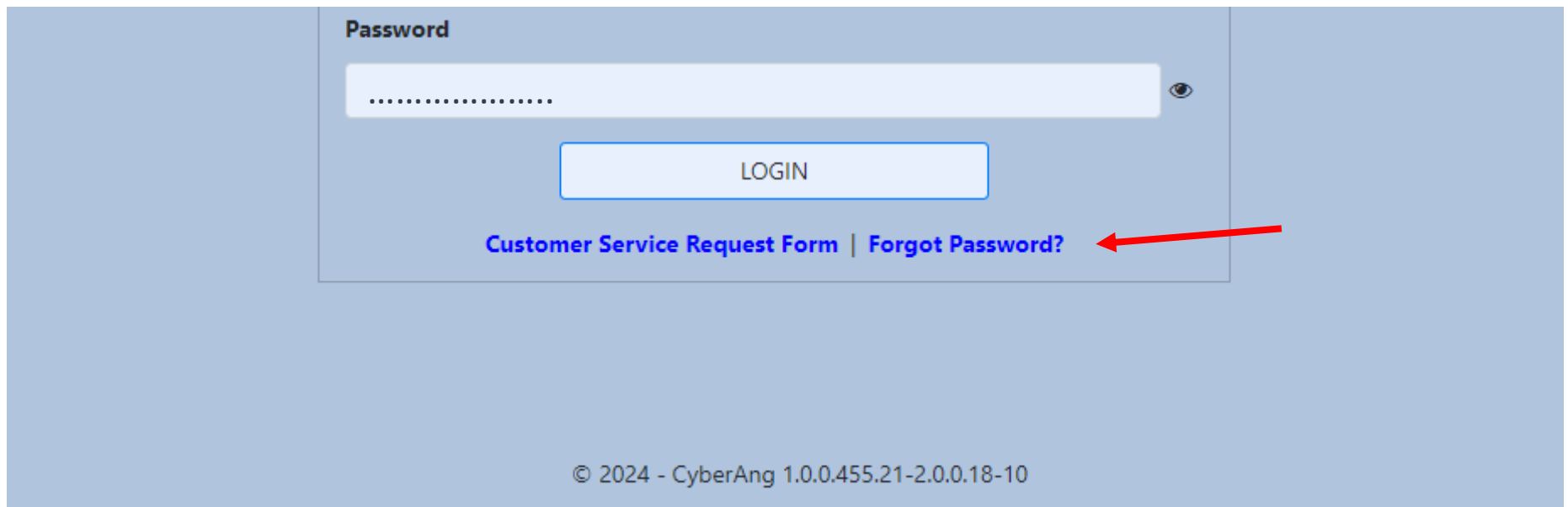
CYBER passphrases do not expire.

You can reset your passphrase if you think your User ID has been compromised, if you have forgotten it, or if you want to change it.

Reset CYBER Passphrase
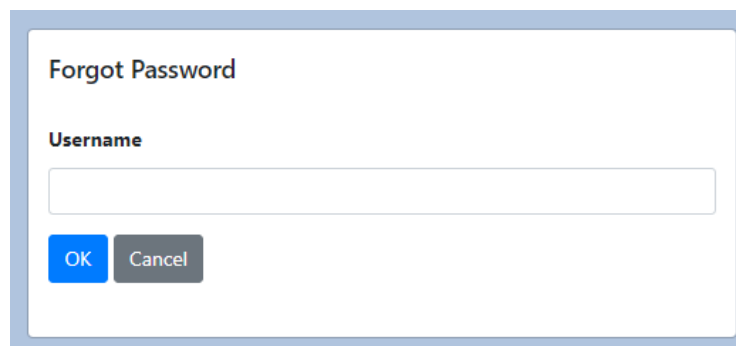
If you forget your passphrase, you can reset it.
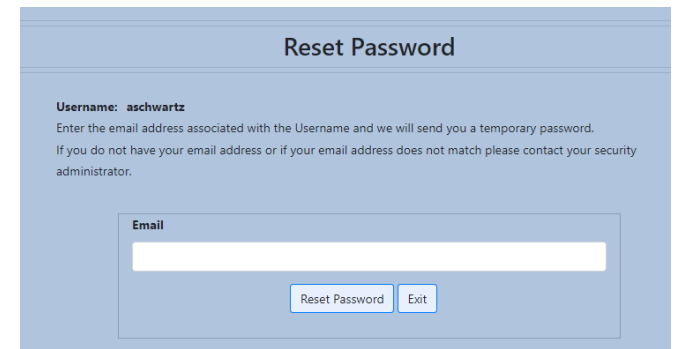
Use the Forgot Password functionality.
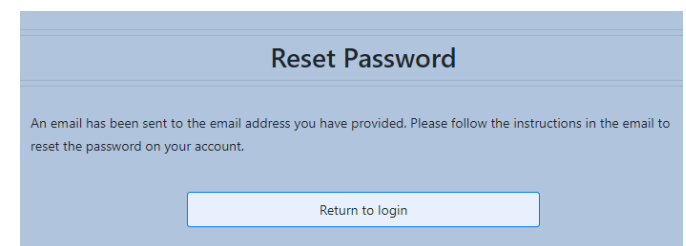
Reset Your CYBER Passphrase on the Login Page

1. Click the **Forgot Password?** link on the CYBER Login Page.

2. The **Forgot Password** screen will open.

3. Enter the UserID and click OK

4. The **Reset Password** screen will appear. Enter your email associated with the ID and click Reset Password.

5. If the correct email is entered, the system will send a temporary passphrase to your email address. Copy the temporary passphrase.

6. Return to the CYBER Login Page and enter your User ID and type or paste the temporary passphrase. Click LOGIN.

7. CYBER will open to the Reset/Change My Password screen.

Reset Password

Username: aschwartz

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.

Email

Reset Password Exit

Forgot Password

Username

OK Cancel

Reset Password

An email has been sent to the email address you have provided. Please follow the instructions in the email to reset the password on your account.

Return to login

Reset/Change My Password

Requirements are listed in RED, and suggestions are in GREEN.

Reset/Change My Password

Enter the Password and click Reset Password to Continue.

Your password:

- Must be at least 20 characters in length.
- The 5 previous passwords cannot be used.
- Using spaces is not recommended.
- May contain UPPER CASE characters.
- May contain lower case characters.
- May contain numbers.
- May contain these characters $ @ # ! ( ) { } [ ] ^ & %

And
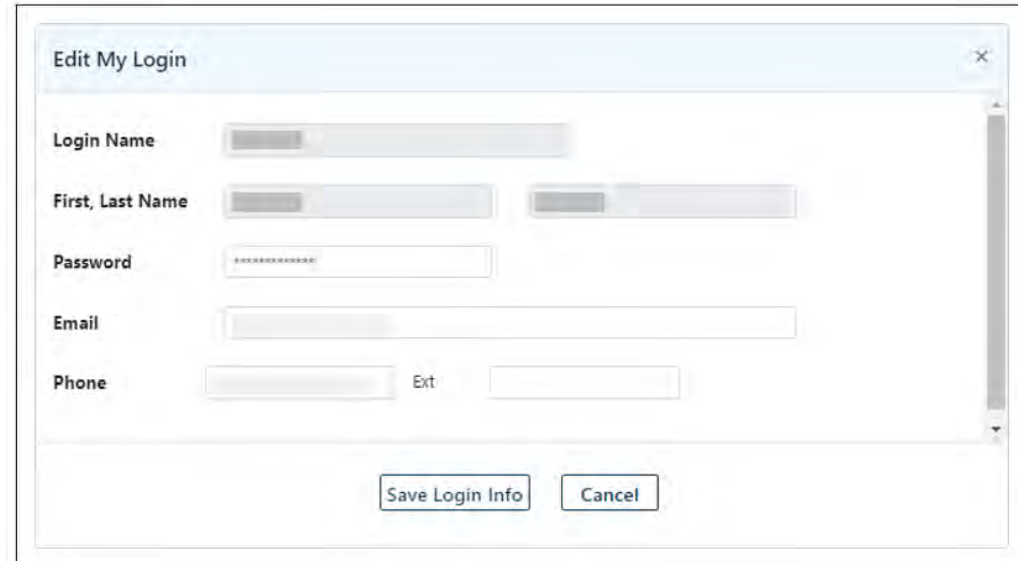
Must match the Confirm password field.

Password

Confirm password

Reset Password   Exit

Reset Passphrase inside CYBER

From the Welcome Page:
- Click System Functions
- Click Manage Access
- **Edit My Login** will appear.

Rules for resetting a passphrase from inside CYBER:

- Must be at least 20 characters in length.

- The 5 previous passwords cannot be used.

- Using spaces is not recommended.

- May contain upper case characters.

- May contain lower case characters.

- May contain numbers.

- May contain these characters: $ @ # ! () { }[ ] ^ & %

Password Security Guidelines

It is extremely important to properly safeguard your passwords.
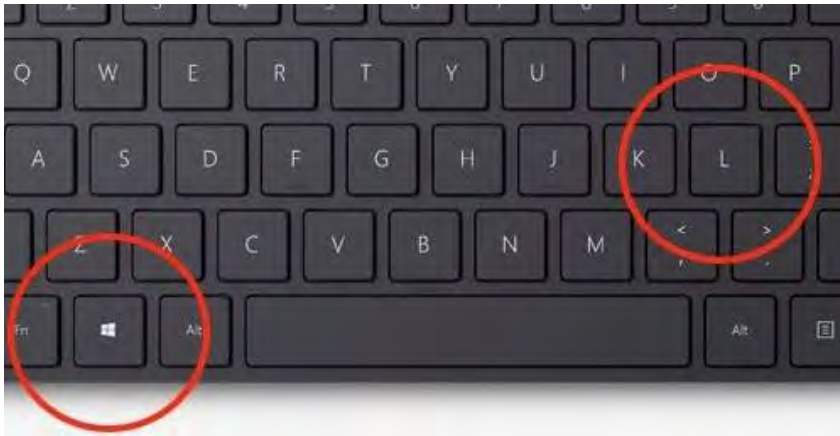
- Do not write down your passwords anywhere.

- Do not store your passwords in an unencrypted document on your computer.

- Never share your passwords with anyone.

- All your passwords should be different*.

*Reusing passwords across different accounts can be risky. If an attacker gains access to one password, they may be able to access your other IDs or accounts.

Computer Security

Take a break from working - Lock your screen!

Never leave your *unlocked* computer unattended at home or in a public place (library, café, airport). It is a security risk!

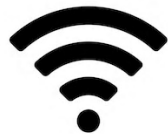To lock a Microsoft screen, click the **Windows Key + L.**

To lock a Mac screen, you can click **Control + Command + Q.**

Public WIFI / Hotspots

Using Public Wi-Fi Hotspots offered at coffee houses, hotels, libraries, airports, are not secure and can allow your data to be accessible to others.

If you need to work in a public space, a better option is to 'tether' or connect your computer to your mobile phone's hotspot *using a cord or cable.*

Using Bluetooth, a mobile phone's hotspot is more susceptible to hacking.

Best Practice Recommendation:
Public networks should never be used when connecting to a sensitive system like CYBER. Work in a private office with a secured network and if available, use a Virtual Private Network (VPN).

Virtual Private Network Options

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network.

The encrypted connection protects data from others accessing or 'listening in'.

Android device, iPhone, or laptop options for VPNs:

1. Use a Browser with built-in VPN settings

2. Your device may have a built-in VPN

3. Use a Third-Party VPN app

What a VPN does is provide a tunnel directly into the site that you want. If anybody listens in along the way, all they pick up is gibberish."

— Herb Lin, senior cybersecurity researcher at Stanford University

Secure Your Home Office

If working from a home office, you should ensure that your office is secure.

- Desk and computer are clear of PHI, screen is not visible to passersby.

- Network is password-secured. (Ethernet cable provides extra security).

- Use headphones when having phone conversations.

- Paper documents are kept in a locked file cabinet or shredded.

- Do not put passwords on Post-It notes!

Add a complex password to your network and change your password routinely!

Network/Computer Been Compromised?

If you are aware that your agency network, CYBER ID 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

CYBER References

For All Users:

- PerformCare Training webpage

- Password Reset for All Providers– guide describes the password reset functionality for all users.

- CYBER Password Reset Functionality – describes the password reset functionality.

- CYBER Password Reset Functionality Presentation Link

- Quick Reference Guide to Secure Email from PerformCare - brief document that describes how to access secure emails from PerformCare.

For Security Administrators:

- CYBER Security Administrator Instructional Guide – detailed guide for security administrators to manage users in CYBER. Includes activation, deactivation, password reset, and all security group descriptions.

- CYBER Security Administrator Quick Reference Guide – brief guide to the most common Security Administrator functions.

Additional References

HIPAA Rule and HITECH Act (*Health Information Technology for Economic and Clinical Health Act)*

- Summary of the HIPAA Security Rule Office of Civil Rights, Department of Health and Human Services. Health Information Privacy. (2024)

- What is the HITECH Act? Alder, Steve. "The HIPAA Journal" (website). (2025)

Care is the **heart** of our **work.**

PerformCARE®