

GREATER COLUMBIA BEHAVIORAL HEALTH Policies and Procedures

Category: Privacy and Security
Approved On: 08/2004
Approved By: The Board of Directors
Revised: 00/00/00
Effective Date: 15 days from approval/ the last revision

No: PS610.00

Title: Password Protection Procedure

GCBH's mission and guiding ethical principal place great value on the privacy and confidentiality information. Beyond these principles, this privacy and security are mandated by state and federal laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA). These regulations require that GCBH deploy and maintain a set of policies, practices, and technologies to safeguard confidential information and ensure that such information is not disclosed to anyone without the proper authorization to view or possess such information.

I. Access Codes and Passwords:

The confidentiality and integrity of data stored on company computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties.

The Information Services department will institute a system of access controls consisting first of a unique identification code and password requirement for each employee with a need to use GCBH computer systems and networks. The characteristics of the password requirement consist of the following:

- A. The password must consist of at least 8 alphanumeric characters from at least three of the following:
 - 1. Upper case.
 - 2. Lower case.
 - 3. Numbers.
 - 4. Special Characters.
- B. The password must be changed by each user at least every 60 days.

II. Information Services Responsibilities:

Policy Title: Password Protection Procedure
No.: SP610.00

- A. The Information Services department shall be responsible for the administration of access controls to all company computer systems.
- B. The Information Services department will deploy and maintain a set of system/network access and password procedures that require unique user identification codes and passwords that conform to the characteristics outlined above.
- C. The Information Services department will maintain a list of administrative access codes and passwords and keep this list in a secure area.
- D. The Information Services department will assign responsibility for maintenance of the access code and password assignment to a qualified individual in the Information Services department. Additionally, a back-up staff person of the department will also be assigned these duties as a backup to the primary staff person.
- E. Set the default to change passwords at least every 60 days.
- F. Set the default so that passwords must consist of at least 8 alphanumeric characters from at least three of the following: Upper case; Lower case; Numbers; Special Characters.
- G. Set the default to activate a password protected screensaver, set for 15 minutes.
- H. Set the default that after three failed attempts to log on, the system will refuse to permit access for 30 minutes.
- I. Set the default for a password history of 18 remembered passwords.
- J. No less than annually, the Information Services department will conduct an audit of the access code and password policy and practice. The results of this audit will be forwarded to the Privacy Officer.

III. Employee Responsibilities:

Each employee:

- A. Shall be responsible for all computer transactions that are made with his/her User ID and password.
- B. Shall not disclose passwords to others. This should be strictly interpreted by all staff. If a password is requested from an employee, the employee should verify the identity of that person with the Information Services department staff member responsible for maintenance of the access codes and passwords. If the responsible staff are not available, the employee is instructed not disclose his/her password.
- C. Passwords must be changed immediately if it is suspected that they may have become known to others. In the event that an employee suspects or knows that his/her password has become known to an unauthorized person, the employee should immediately report this event to the following agency staff:
 - 1. The designated staff person in the Information Services department responsible for maintenance of access codes and passwords
 - 2. The Privacy Officer

- D. Passwords should not be recorded where they may be easily obtained. Employees shall not display passwords in any area that can be viewed by others. This means practically that passwords should not be written on “sticky” notes on the monitor, placed on paper and taped to the bottom of the keyboard, etc.
- E. Will change passwords at least every 60 days.
- F. Should use passwords that will not be easily guessed by others.
- G. Should log out when leaving a workstation for more than 30 minutes or when leaving the premises for any length of time.
- H. Should have a password protected screensaver set for 15 minutes.

IV. Emergency Access to Applications:

An emergency may arise in which a user needs access to a system resource that is password-protected under another user ID and where that particular user is unavailable. In no circumstance should the original user ID-account owner’s password be shared to access the application. In order to have a clear chain of responsibility, the IS Manager will reset the resource owner's password and reassign the account to another individual (thereby transferring responsibility for actions performed by that particular userID).

V. Managers’ Responsibility:

Managers should notify the Information Services department promptly whenever an employee leaves the company so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

VI. Enforcement:

All managers are responsible for enforcing this procedure. Employees who violate this procedure are subject to discipline up to and including termination from employment in accordance with GCBH’s Sanction Policy.

VII. Scheduled Review of this Policy:

The review of the GCBH policies and procedures manual is on a two year cycle. The GCBH policy review and revision approval process is a three month process. This policy is scheduled to be reviewed every second year:

- A. by GCBH staff by April of odd years,
- B. by the Regional Advisory Board (RAB) by May of odd years,
- C. by the GCBH Board of Directors by June of odd years, and
- D. outside of the schedule if required.