

# GREATER COLUMBIA BEHAVIORAL HEALTH

## Policies and Procedures

Category: Privacy and Security  
Approved On: 03/27/2003  
Approved By: The Board of Directors  
Revised: 00/00/00  
Effective Date: 15 days from approval/ the last revision

**No: PS606.00**

**Title: Computer and Information Security Policy**

### **I. Introduction:**

- A. Greater Columbia Behavioral Health (GCBH) has adopted this policy to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as well as with our responsibility to safeguard the confidentiality and integrity of protected health information (PHI) as required by law, and professional ethics. Familiarity with the policy is an important part of every employee's responsibilities.
- B. Because much of GCBH's confidential information is stored in electronic computer networks and devices, GCBH must take great care to ensure that access to those computers, networks, and devices is strictly limited to staff with a need to know and/or view that information. The key elements of GCBH computer and information use are included in the following procedures:
  - 1. Workstation and Portable Computer
  - 2. Password Protection
  - 3. Remote Access
- C. GCBH makes use of access codes and passwords. The Password Protection Procedure outlines the specific policies and procedures for management of those codes and passwords. All users are expected to be familiar with and comply with this procedure.
- D. GCBH staff using computer terminals, laptop, notebook, or other portable computers must be familiar with and follow the contents of the Workstation and Portable Computer Procedure.

## **II. Workstation Use Assumptions:**

- A. Every computer workstation in GCBH is vulnerable to environmental threats, such as fire, water damage, power surges, and the like.
- B. Any computer workstation in GCBH can access confidential information if the user has the proper authorization.
- C. All computer screens can be visible to individuals who do not have access to confidential information that may appear on the screen.

## **III. Portable Computer Assumptions:**

- A. Portable computers pose a significant security risk because they may contain confidential information and, being portable, are more at risk for loss, theft, or other unauthorized access than GCBH's less easily movable computers.
- B. Portable computers may be more vulnerable to viruses and other such threats because the user may not regularly use virus protection software and other electronic safeguards the way the agency's Information System Manager does on the agency's network.
- C. Portable computer use is more difficult for GCBH to audit; thus security breaches may be more difficult to identify and correct.

## **IV. Preventative Measures for Workstations and/or Portable Computers:**

- A. GCBH staff will monitor the computer's operating environment and report potential threats to the computer and to the integrity and confidentiality of data contained in the computer system. For example, noise level increase, virus, or other such attacks.
- B. All computers plugged into an electrical power outlet will use a surge suppressor approved by the Information Services Manager.
- C. GCBH staff shall take appropriate measures to protect computers and data from disasters.

## **V. Remote Access:**

Remote access is meant to be an alternative method of support for GCBH office functions. By using GCBH hardware, software, and/or network systems you assume personal responsibility for their appropriate use. Staff is expected to read and comply with the Remote Access Procedure, and to understand the following:

- A. That any software and hardware devices provided to you by GCBH remain the property of the Agency.

- B. Not to modify, alter, or upgrade any software programs or hardware devices provided to me by GCBH without the permission of the Information Services Department.
- C. Take maximum precautions to prevent unauthorized access and/or viewing of client's protected health information.
- D. Strictly prohibited from downloading, copying, or keeping in any form protected health information (PHI) on personal computer(s).
- E. Shall not copy, duplicate (except for backup purposes as part of your job), or allow anyone else to copy or duplicate any software.
- F. If staff leave GCBH for any reason, immediately return the original and/or copies of any and all software, computer materials, or computer equipment received from GCBH that is either in immediate possession or otherwise directly or indirectly under their control.
- G. Understand and agree that reasonable efforts to protect all GCBH provided software and hardware devices from theft and physical damage must be taken.

#### **VI. Confidentiality and Security Agreement:**

The Confidentiality and Security Agreement (PS605) is used to acknowledge receipt of, and compliance with, this policy. Please read the policy and the agreement. Sign and date the agreement in the spaces provided, and return the agreement (only) to the Information Services Manager. The signed Confidentiality and Security Agreement will be placed in the employee's personnel file.

#### **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.