

# 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/ last revision

**No: PS609.00**

**Title: Remote Access Procedure**

Remote access is a generic term used to describe the accessing of the computer network by individuals not located at the organization's primary office. This may take the form of traveling employees, employees who regularly work from home, or employees who work both from the office and from home. In many cases, both GCBH and the employee may benefit from the increased flexibility provided by a remote access program. As with any innovation, however, the benefits may be countered by risks if the purposes and methods of the program are not fully understood by all participants.

*To optimize the efficiency of our remote access program, we have created a clear policy governing eligibility, obligations and responsibilities of remote users.*

Participation in a remote access program may not be possible for every employee. Remote access is meant to be an alternative method of meeting GCBH needs. The Agency may refuse to extend remote access privileges to any employee or terminate a remote access arrangement at any time.

GCBH procedures for remote access are as follows:

## **I. Acceptable Use:**

Hardware devices, software programs, and network systems purchased and provided by GCBH for remote access are to be used only for creating, researching, and processing Agency-related materials. By using GCBH hardware, software and network systems you assume personal responsibility for their appropriate use and agree to comply with this policy and other applicable policies, as well as City, State and Federal laws and regulations.

## **II. Equipment & Tools:**

GCBH will provide tools and equipment for remotely accessing the corporate computer network in a secure manner. This may include computer hardware, software, phone lines, e-mail, voicemail, VPN hardware and software, connectivity to host applications, and other applicable equipment as deemed necessary.

The use of equipment and software for remotely accessing the computer network is limited to authorized persons and for purposes relating to GCBH business. GCBH will provide for repairs to their equipment. When the employee uses her/his own equipment, the employee is responsible for maintenance and repair of equipment.

## **III. Password and Privacy Protection:**

By using GCBH hardware, software and network systems you assume personal responsibility for their appropriate use and agree to comply with GCBH Password Protection policy. In addition, the employee agrees to take maximum precautions to prevent unauthorized access and/or viewing of client's protected health information during remote access sessions. To do this, employees must agree to place the computer in a secure environment (not in open living rooms or other common spaces) and to log-off of the GCBH network when absent from the computer.

## **IV. Use of Personal Computers and Equipment:**

There are literally thousands of possible interactions between the software needed by the remote user and the average mix of programs on most home computers. Troubleshooting software and hardware conflicts can take hours, and can result in a complete reinstall of operating systems and application software as the only remedy for problems. For that reason the Information Services department will only provide support for equipment and software provided by GCBH.

If the employee's personal computer does not have anti-virus software, GCBH will provide such to the employee. The employee agrees to install and maintain this software along with any virus definition updates that are issued.

Because of the fluid nature of software development and security patches, the employee agrees to install and maintain any and all software patches issued by the Information Services department. GCBH will bear no

responsibility if the installation or use of any necessary software causes system lockups, crashes, or complete or partial data loss. The employee is solely responsible for backing up data on their personal machine before beginning any work. At its discretion, GCBH will disallow remote access for any employee using a personal home computer that proves incapable, *for any reason*, of not working correctly with GCBH-provided software, or being used in a production environment. If the employee has a critical need for remote access and the employee's personal computer(s) is unsuitable for the task, the employee should submit a formal request for GCBH equipment to be provided. This request should flow through the employee's Manager to the Information Services Manager, who in turn will notify the Privacy Officer.

Because of the extreme security and privacy risks associated with the use of remote access and personal computers, employees are strictly prohibited from downloading, copying, or otherwise keeping client's protected health information on personal computers.

#### **V. Enforcement:**

Penalties for violation of the Remote Access Procedure will vary depending on the nature and severity of the specific violation. Any employee who violates the Remote Access Procedure will be subject to discipline up to and including termination from employment in accordance with GCBH's Sanction Policy.

#### **VI. 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 procedure 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.