

GREATER COLUMBIA BEHAVIORAL HEALTH Policies and Procedures

Category: Management Information System
Approved On: 02/24/2001
Approved By: The Board of Directors
Revised: 04/22/2004, 01/10/2005, 02/23/2006
Effective Date: 15 days from the last revision date

No: IS702.02

Title: Network Security Policy

I. Purpose:

This policy is designed to address security related items to ensure the integrity of data and the privacy of our consumer data from unauthorized access

II. Process/Procedures:

The below list are the minimum requirements implemented throughout the region.

- A. Ensure that the event viewer and security logs are activated on all computer servers, and desktop computers where applicable.
- B. Ensure that all computer servers and applicable workstations are backed up at least weekly.
 - 1. Applicable workstations are those machines that house data files not located on the server. An effort should be made to keep data files as centralized as possible.
 - 2. A backup log can be printed out of most software, which include date and time stamps.
 - 3. A suggestion to do incremental backups between a full data dump.
 - 4. Test backup tapes monthly.
 - a. This should be done by a different person than the one doing the backups.
 - b. This can be accomplished in a small time frame by choosing one small file and restoring it.
- C. A method must be in place to ensure that workstations can be restored to their fundamental operation quickly. An example of this would be to ensure that emergency repair disks for all pc's are available or shadowing software (i.e.,

Ghost, Disk Image, etc.) are in use. Computers and laptops need to be supportable for security (physically and electronically).

D. Virus and malware protection to be installed, kept up-to-date, and running on all computers and servers including the e-mail server.

1. The virus and malware protection software that is chosen should have the capability for timely upgrades.
2. Most virus and malware software have access to signature files/upgrades on the product home page.

E. Every effort must be made to prevent unauthorized access of data. All desktop computers to be password protected, and screen savers activated. In addition, computer monitors and printers should be located as to eliminate unauthorized viewing.

1. Minimum standards shall be:

- a. Set the password to eight alphanumeric character minimum, from at least three of the following;
 - i. Upper case.
 - ii. Lower case.
 - iii. Numbers/special characters.
- b. Lockout after three bad attempts (for thirty minute duration, or administrator intervention);
- c. Set the password to be changed by each user to at least every ninety days;
- d. Set a 5 password history (forces users to choose a different password);
- e. Screensavers to be active and password protected (after 30 minutes);
- f. Do not post password on or near workstation.

F. Floppy disks, memory keys, and other removable media and hardware should not be left out unsecured, and any PHI on these devices should be encrypted or password protected.

G. Disaster Recovery Plan (HIPAA and BBA compliant) in place.

H. Portable systems (i.e., laptops, palm pilots, handhelds) stored securely.

I. Computers, laptops, memory keys/removable media, and servers are cleaned of Protected Health Information (PHI) before reassignment or surplus.

- J. The server room should be kept as secure as possible.
 - 1. The door should be closed and locked with minimal key distribution only to authorized personnel.
 - 2. Unused keys should be secured.
 - 3. A log review conducted periodically of key disbursement.
 - 4. A maintained air temperature as per server requirements.
 - 5. Network devices (i.e., hub, wireless access, router, etc.) located in server room or secured area.
 - 6. Uninterrupted Power Supply or backup generator in use.
 - 7. Fire extinguisher checked and rated for electrical fires dedicated to server room.
- K. A Firewall is used on all networks.
- L. Wireless Access Points and networks, if used, are secure.

These are minimum security requirements, agencies can have more restrictive standards.

III. 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 July of odd years,
- B. by the Regional Advisory Board (RAB) by August of odd years,
- C. by the GCBH Board of Directors by September of odd years, and
- D. outside of the schedule if required.