SOUTHERN HIGHLANDS COMMUNITY MENTAL HEALTH CENTER

POLICY AND PROCEDURE MANUAL

Date of Issue: 10/2/07 **Section Number 412**
Date Revised:

Policy 412 – Data Backups and Contingency Planning

I. POLICY

It is the policy of Southern Highlands Community Mental Health Center to provide reliable and redundant backups and disaster recovery of a system and user generated data on each of the systems which it administers.

II. PURPOSE

The purpose of this policy is to provide backup and a disaster recovery plan in case of an event.

III. PROCEDURE

BACKUPS

The Systems Manager will name a primary and backup staff member to perform the system backups for each system.

1. Full system backups are performed on a daily basis (Monday thru Thursday) on all multi-user systems managed by the IT Department.
2. Full system backups are performed on a weekly basis (Friday).
3. Full system backups are performed on a monthly basis (last day of the month).
4. Full system backups are performed on an annual basis. This backup is completed at the time the current fiscal year is closed.
5. Each backup will be verified either by a list or a log file.
6. A calendar listing the backups will be maintained for each system.
7. The Thursday backup will be kept offsite and maintained at 325 Mercer Street.
8. Bootable backups are performed monthly.

BACKUP STORAGE

1. The daily backup tapes will be rotated on a monthly basis.
2. Annual backups will be maintained for 10 years.
3. All backups will be stored in the IT Department in a fireproof safe.

USER BACKUP RESPONSIBILITIES

1. Users are responsible to backup all information in their specific password protected file on the server.
2. Users will not save EPHI on any floppy disk, CD, or hard drive on their computer.

DISASTER RECOVERY

1. All computer systems managed by Southern Highlands CMHC are included in a general insurance policy.
2. The computer systems are monitored daily by the IT Department.
3. All servers are powered by an Uninterruptible Power Supply (UPS) which can maintain full power to the servers until they are powered off.
4. A bootable tape and the vendor software are stored in a fireproof safe in the IT Department along with full system backups.