**TITLE:** Record Storage and Security of Protected Health Information

**Policy Number:** AM-HP-003

## STATEMENT OF PURPOSE:

To establish a policy and procedure for the storage of medical information to ensure its security and protection in accordance with the Health Insurance Portability and Accountability Act (HIPAA) and privacy rights related to Protected Health Information (PHI).

## POLICY:

Neighbor To Family protects the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements. Storage of PHI shall be done in a manner that ensures the information is secure and protected at all times.

All supervisors are responsible for enforcing this policy. Individuals who violate this policy will be subject to the appropriate and applicable disciplinary process, up to and including termination or dismissal.

## PROCEDURE:

All personnel must strictly observe the following procedure relating to the storage of PHI:

1. Neighbor To Family personnel must clean desks and working areas (i.e., fax, copier, printer, scanner, etc.) such that all PHI is properly secured, unless the immediate area can be secured from unauthorized access;
2. Departments or units that store PHI in paper format, including client records, must maintain the PHI in locked file rooms or cabinets;
3. When not in use, PHI must always be protected from unauthorized access. When left in an unattended room, such information must be appropriately secured;
4. When PHI is being released through teleconference or video feed, Neighbor To Family personnel must treat the protection of PHI in the same manner as PHI recorded on paper, thereby securing access to the teleconference or video to authorized personnel only;

5. If PHI is to be stored on the hard disk drive or other internal components of a personal computer or PDA (Personal Digital Assistant), it must be protected by either a password or encryption. Unless encrypted, when not in use, this media must be secured from unauthorized access; and
6. If PHI is stored on diskette, CD-ROM, or other removable data storage media, it cannot be commingled with other electronic information. Storage media must be maintained in locked file rooms or cabinets.

Standards for Storage and Security of Off-Site Locations

1. Neighbor To Family prohibits the unauthorized disclosure of PHI while in use at Neighbor To Family or while in use at any off-site location. Whenever a hard copy version of PHI (actual client records, photocopies, and extra printouts) is removed from Neighbor To Family premises, it must be secured and protected at all times.
2. Client records, case management records, source data and any other information that contains PHI may not be removed from Neighbor To Family premises unless there has been prior approval from the custodian of the information. In some instances, the removal of case management records and other PHI may require documentation and tracking. This policy applies to PHI in any form, including electronic PHI, held by a Neighbor to Family facility.
3. When employees use PHI at home, the information should be stored in a secure manner so no other individuals in the home will have access to the PHI. For example, the information should be locked in a file drawer or briefcase when not in use. If Neighbor To Family computers or individual home computers are used to store PHI, the PHI must be stored and protected from any and all unauthorized access.
4. All PHI must be returned to Neighbor To Family. PHI should be returned to the custodian who granted the Neighbor To Family employee permission to remove the PHI.