CONFIDENTIALITY AND PROTECTED HEALTH INFORMATION
Community Friendship, Inc.

The Health Insurance Portability and Accountability Act (HIPAA) was signed into federal law in 1996 by President Clinton with the intent of protecting workers and their families with health insurance coverage should they become unemployed. Congress saw this as an opportunity to simplify the administrative aspects of health insurance in an effort to reduce health care costs by restructuring the way health information is transmitted, captured, stored and secured. Protection of patient privacy and standardized security are two of the requirements in this Administrative Simplification that have an impact on Community Friendship, Inc. (CFI).

CFI policies and practices have always stressed the importance of controlling the release of confidential information and the importance of maintaining confidential information in a manner that is safe and protected. HIPAA defines **Protected Health Information** (PHI) as "individually identifiable health information that is maintained or transmitted by a covered entity. Health information is information, whether oral or written, communicated in any medium that relates to an individual's health condition, provision of health care to an individual, or payment for such health care." HIPAA regulations make it more important than ever that we maintain an awareness and practice behaviors that exhibit strict adherence to confidentiality and privacy.

Below are a few general guidelines regarding protecting confidential information:

- **Maintain the confidentiality, security and integrity of consumer or agency information**. It is not acceptable and considered a violation to access, view, modify, destroy or disclose information in any medium (verbal, written, electronic, etc.) without authority.
- **Do not disclose confidential information out of carelessness or neglect**.
    - Do not discuss a consumer in a public or inappropriate area (the lobby, cafeteria, staff mailboxes, an office shared by multiple staff, etc.).
    - Do not leave confidential information in a public area within the view of others (leaving clinical records unattended in an unlocked office, in a meeting room, board room, etc.).
    - Do not leave a computer unattended if confidential information is unsecured.
    - All transportable media (flash drives, disks, etc.) or email that contains confidential information should be password protected.
    - Do not discard confidential information without shredding it.
- **Do not access or disclose information out of curiosity or concern without authorized need to know**. One example would be looking up information on a friend, relative or accessing consumer information out of concern or curiosity rather than a work related need to know.
- **Do not access, review, change, destroy or disclose confidential or agency information for personal gain or with malicious intent**. Examples would be

using confidential information in a personal relationship, accessing information to be sold or shared with others for mailing lists, etc.

Staff should report violations of confidentiality to CFI's Privacy Officer. CFI will not retaliate against you for filing a complaint. When allegations are found to have merit, disciplinary action will be commiserate with the severity of the violation. You may contact CFI's **Privacy Officer by telephone at (404) 875-0381 , facsimile (404) 875-8248 , or by mail to 85 Renaissance Parkway, Atlanta, Ga. 30308** for further information.

Be aware that civil and criminal penalties can apply to you individually for failure to comply with privacy regulations.

Revised July 2014