HILLTOP

Creating Opportunities. Enriching Lives.

Hilltop Community Resources

ALL EMPLOYEE

HIPAA Policies and Procedures

Updated 11/11/2018

I. Purpose of Policy

Hilltop recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations and has adopted this General HIPAA Compliance Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA").

Hilltop acknowledges our duty and responsibility to protect the privacy and security of the following personal identifiers, including, but not limited to; Name, Social Security Number, Date of Birth, Address; Admit Date, Telephone Number or any other identifying number or symbol (e.g., insurance or medical record number).

You might hear and see "*personal identifiers"* referred to as:

- Protected Health Information (PHI)
- Electronic Protected Health Information (ePHI)
- Protected Identifying Information (PII)
- Individually Identifiable Protected Information (IIPI)
- Individually Identifiable Health Information (IIHI)

We also acknowledge our duty and responsibility to support and facilitate the timely and unobstructed flow of health information for lawful and appropriate purposes.

It is important to understand that in our work at Hilltop ALL employees are responsible for protecting the privacy of any personal identifiers that can be connected to any of Hilltop's residents or clients. *See Confidentiality Policy in Hilltop's Employee Handbook*.

II. Basic Protections & Safeguards

All Hilltop employees must reasonably safeguard personal identifiers from an intentional or unintentional use or inappropriate disclosure.

The following information will cover Hilltop employee responsibilities to maintain the Privacy and Security of personal identifiers.

a. Physical Safeguards

Physical measures are policies, procedures, or other measures taken to protect an organization's electronic information system, related buildings, and equipment from natural and environmental hazards, or an unauthorized intrusion.

Hilltop employees are required to protect all PHI/ePHI in their possession by safeguarding the information. This can be done by following these guidelines:

- **i.** Lock computer workstations when away from desk (CTRL+ALT+DELETE) or ("Windows Key" + L).
- **ii.** Lock up portable devices such as laptops, cell phones, or tablets.
- **iii.** Put paper documents away in a locked filing cabinet or desk drawer when away from work area.
- **iv.** Do not forward work emails to personal email accounts.
- **v.** Do not upload information to unauthorized websites.
- **vi.** Do not leave documents on printers and faxes.
- **vii.** If sending interoffice mail use confidential envelope.
- **viii.** All files containing personal identifiers, that no longer need access, will be kept in a secure location, either on premises or at a secure facility, available only with authorization from a Program Director or member of Senior Leadership.

b. Technical Safeguards

Technical safeguards, as well as the policy and procedures for its use, designed to protect personal identifiers and control access to it, include:

- **i.** Do not share your unique user ID's and passcodes.
- **ii.** Assure email encryption on outgoing and incoming email correspondence.
  - Emails between Hilltop employees are protected automatically.
  - Use secure email by typing **secure.htop** in the email subject line.

- If you receive PHI via email, it is your responsibility to request all future emails be encrypted.

iii. Follow Hilltop's Information and Communications Systems Policy, which can be found in the Employee Handbook.

III. Follow the KYSS Rule

KYSS = KEEP YOUR STUFF SECRET!

KYSS guidelines:

- Refrain from gossip or chit-chat regarding clients, co-workers, and their situations.
- Keep confidential conversations within the supervisor/employee relationship.
- Maintain strict confidentiality of client records and documentation.
- Avoid correspondence that does not relate to business or serves no valid business purpose.

IV. Breach Notification

a. *Breach* means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under HIPAA regulation.

b. If you suspect or know a breach of information has happened it is important to let your supervisor or the Privacy Officer know right away.

c. The Privacy Officer, in conjunction with the Program Director and other Officers, will review, develop and implement an appropriate Plan of Correction for the level of breach, which has occurred.

V. Release of Information

a. No information shall be released to any outside individuals or agencies without a properly signed Release of Information form or appropriate court order. Prior to responding to requests for client information or action, including requests for information from process servers, search warrants, investigators, or attorney requests, employees should consult immediately with their Program Director for direction on the appropriate response.

VI. Violations of Policy

a. This policy governs disciplinary actions for Hilltop. All personnel of Hilltop must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce. Hilltop must comply with HIPAA and the HIPAA implementing regulations pertaining to employee sanctions.

b. It is the Policy of Hilltop to document, establish and implement appropriate, fair and consistent disciplinary actions for employees who fail to follow established policies and procedures, or who commit various offenses.

c. Disciplinary actions applied shall be appropriate to the nature and severity of the error or offense, and shall consist of an escalating scale of sanctions, with less severe sanctions applied to less severe errors and offenses, and more severe sanctions applied to more severe errors and offenses.

HIPAA does not apply to workers compensation insurers, workers' compensation administrative agencies, or employers.

CONTACT INFORMATION:

Security Officer / Privacy Officer:
Carter Bair
970-244-0403
carterb@htop.org

Ethics Officer:
Ali Weatherby
970-244-0630
aliw@htop.org

Compliance Officer:
Will Hays
970-244-0450
willh@htop.org

Information Technology Officer:
Debbie Aull
970-244-0431
debbiea@htop.org

People Operations Department
970-242-4400
peopleops@htop.org