FOOTHILLS GATEWAY, INC

Health Insurance Portability and Accountability Act (HIPAA)

POLICY:

It is the policy of Foothills Gateway, Inc. to comply with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) 45 CFR Part 164 and any subsequent revisions or additions.

PROCEDURE:

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law (Public Law 104-191). Within HIPAA are Security Standards to protect the confidentiality, integrity and availability of electronic protected health information. Foothills Gateway, Inc. (FGI) serves individuals whose protected health information (PHI) is confidential. Payment for services is obtained through electronic transfer of PHI. FGI will maintain compliance with HIPAA.

Committee

A HIPAA Committee will meet as needed to review HIPAA standards in relation to established FGI policy and procedures. The committee will initiate new procedures, request update of existing procedures, modify formats, train staff, and take other steps to maintain compliance with the HIPAA Act of 1996.

Members of the committee will include the Chief Administrative Officer, Chief Operating Officer-Services, Comprehensive CM Director/PCT Trainer, Support Services CM Director/PCT Trainer, Information Technology Director, and the Placement Coordinator.

Privacy Officer, Security Officer and Complaint Officer

Specific FGI staff will be assigned the responsibilities of Privacy Officer (Chief Administrative Officer), Security Officer (IT Director) and Complaint Officer (Chief Operating Officer-Services). The Privacy Officer is responsible for the development and implementation of the HIPAA policies and procedures at FGI. The Security Officer is responsible for the implementation of the policies and procedures required for security of PHI at Foothills Gateway. The Complaint Officer is responsible for receiving complaints and providing further information.

Notice of Privacy Practices

The FGI Privacy Practices Notice outlines the uses and disclosures of protected health information, individual rights, and the responsibility of FGI to safeguard protected health information and to comply with the Breach Notification Rule as appropriate.
Individual rights included in the Notice of Privacy Practices include

- Right to Privacy Protection for PHI.
- Right to request restriction on uses and disclosure.
- Right to access individual PHI.
- Right to amend PHI.
- Right to an Accounting of Disclosures of PHI for up to six years.

- Right to be notified in the event of a breach of unsecured PHI.

The Notice of Privacy practices is posted at FGI, and in FGI operated residential home sites within the community. Copies of the notice are also on the FGI website and are available upon request. The Notice of Privacy Practices is available in English and Spanish.

The Notice of Privacy Practices is sent to all individuals receiving services, guardians, and/or family members at the time of original eligibility and/or upon admission to services. An acknowledgment of receipt of the notice is to be signed, returned to FGI and filed in the individual master file. The Notice of Privacy Practices is also included with copies of the annual Service Plan.

Business Associate Contracts

The HIPAA Committee with assistance from the Finance Director will identify all Business Associates of FGI. A Business Associate is a person or business that needs access to or receives protected health information concerning individuals receiving services in order to perform services for FGI. HIPAA Compliance standards and the Breach Notification Rule are included in the Business Associate Agreement to assure the Business Associate will safeguard all received protected health information. (Refer to Business Associate Agreement.) Business Associate Contracts originating from FGI are updated as needed and maintained in the finance department. All Business Associate Contracts are signed by the appropriate Chief Officer at FGI.

Staff Training

All FGI staff, volunteers, and committee members receive training about the HIPAA law and how it integrates with confidentiality expectations and methods of using PHI at FGI. New staff will receive HIPAA information as part of the Module I Training. All staff will review and sign off on the HIPAA policy every year. In addition, supervisory staff will be trained annually. Non-supervisory staff will be trained every other year.

FGI staff violating HIPAA standards will be subject to disciplinary action.

Compliance Measures

If a violation occurs:

- The supervisor will request the staff member to complete a Confidentiality Error form for internal errors, or the HIPAA Breach Risk Assessment if it is a possible breach.
- The supervisor will then email the HIPAA Privacy Officer, the Placement Coordinator, and the Chief Officer of their division to notify them of the error/violation.
- The supervisor will consult with the HIPAA Privacy Officer or designee, as needed, to determine the level of risk and/or type of error. In addition, a determination will be made as to whether a possible breach of PHI occurred. The Placement Coordinator will provide backup and assistance as needed for this step.
- The supervisor and employee will discuss methods of preventing further confidentiality errors. The form will be signed and dated by the staff person,

supervisor, Privacy Officer and the Chief Officer, and then filed in the employee personnel file.

- Confidentiality errors will be taken into consideration at the annual performance evaluation in relation to the individual job responsibilities.
- Confidentiality errors are tracked by the Privacy Officer or designee.

- If a HIPAA breach did occur:
  1. Breaches will be reviewed by the HIPAA Committee and the appropriate individuals and Health and Human Services will be notified to comply with the Breach Notification Rule.
  2. Breaches are logged into a tracking system maintained by the Human Resources Office.
  3. Based on the unique circumstances of the breach, the Department of Health and Human Services (HHS) will be notified immediately or the breach will be included in the annual reporting to HHS.

Levels of Access

A Level of Access is assumed for each staff position at FGI. Levels of Access will be based on the staffs' need to know in order to perform their job duties.

Location of Protected Health Information

The HIPAA Task Force will identify the location of all PHI and determine appropriate safeguards to prevent unauthorized disclosure.

Staff Expectations

- Staff will not share their network passwords with anyone other than their direct supervisor or IT staff.
- Staff will safeguard the disclosure of protected health information in the community, and throughout the agency program areas and/or residential sites.
- All discarded papers, documents, letters, or files to be destroyed containing protected health information must be placed in enclosed recycle bins placed throughout FGI. All paper in the recycle bins will be shredded for disposal.
- Sign-out sheets at the front desk will only give a person receiving services initials or first name.
- Staff will cover all lists, calendars and other organizational materials containing protected health information to avoid incidental disclosure.
- Staff will follow the confidentiality policy and procedure concerning accessing, using, and releasing protected health information about a person receiving services.
- Conversations between staff members concerning individuals receiving services will be held in private offices or rooms, and not in areas of the building generally accessed by the public.
- Protected health information sent by Fax will contain a disclaimer stating the information is intended only for the individual named on the Fax cover sheet. Refer to Fax cover sheet.
- A disclaimer message is included with all outgoing email messages

Authorization for Release of Information

Protected health information about a person receiving services will be shared only after obtaining a Release to Share Information form signed by either the individual receiving services, parents of a minor, guardian or authorized representative. The authorization for release must be specific to the type of information to be shared, the person or agency receiving the information, and purpose for disclosure. The authorization will be dated and can only be effective for a one-year period.

Individuals receiving services, parents of a minor, guardians and/or authorized representatives can also deny access to their protected health information by signing a denial of access form.

An authorization for release of Information is not required when protected health information will be used for the purposes of treatment, payment for services or health care operations.

Disclosure of protected health information will be tracked in the Service Plan (SP) tracking system to facilitate reminders to renew the authorization every year as necessary.

Definitions

Protected Health Information: Individually identifiable health information transmitted by electronic media, maintained in any medium that is defined as electronic media, or transmitted or maintained in any other form or medium. Information created or received, relating to past present or future physical or mental health of an individual.

06/04. . . . . 1/11; 5/12; 1/14; 12/15; 2/16; 9/16; 2/18