MEDICAL RECORD INFORMATION CONFIDENTIALITY

PURPOSE

To ensure the confidentiality, security and integrity of information in accordance with applicable federal and state laws and regulations.

POLICY

Agency will observe the patient's/client's right to confidentiality of information and will implement processes that ensure this confidentiality. This includes provisions of the Privacy Rule of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996, as well as other Federal and State regulations and their revisions, as applicable.

PROCEDURE

I. Access To Information

A. Upon admission to Agency, each patient/client will have a medical record established.

B. Before assuming job responsibilities, all staff will be educated regarding the confidential nature of medical records, including provisions of HIPAA, and information and be informed of the resulting disciplinary action for willful, unauthorized disclosure of confidential information, up to and including termination.

1. If the Agency changes its policies and procedures related to confidentiality, security and integrity of information, all employees shall receive retraining.

2. All privacy orientation and retraining shall be documented in the employees' personnel files.

3. The Privacy Officer shall maintain a record of privacy training given to the employees as defined in the Privacy Rule.

C. Agency staff will have access to the minimum amount of patient/client health information necessary to perform their duties as described below:

1. Per-visit staff - access to all information 24 hours a day, 7 days a week.

2. Administrative staff - access to all information 24 hours a day, 7 days a week.

3. Quality assessment/improvement staff - access to all information during office hours.

4. Billing staff - access to information needed to process claims during office hours.

5. Clerical staff responsible for chart maintenance or data entry - access to information for inclusion in medical record for copying, filing, data entry, and retrieval to use in the course of their assigned duties.

6. Visiting staff - at request of administration, access to all information during office hours.

7. If an employee has more than one job title, he/she shall have access only in the capacity he/she is functioning at the time.

D. Any discussion involving patient/client/caregiver information will be conducted discreetly to avoid accidental disclosure to unauthorized persons.

E. Patient/client computer data will be accessed, entered, or retrieved by authorized persons only.

F. All employees who have access to the system will be given network and patient/client database username and passwords. These passwords are not to be shared with any person. Passwords will be changed by the user at least annually, recommend quarterly or following a breach in security. Passwords will be deleted at termination of an employee.

G. Measures such as locking file cabinets or locking the medical record room will be utilized for protection of records from access and/or retrieval by unauthorized personnel after office hours.

H. Other sources that may have access, without patient/client consent, are:

1. Payor sources;

2. Contracted billing companies who are bill via electronic claims;

3. Regulatory agencies;

4. Accrediting bodies; and

5. Contracted consultants.

I. Any information needing to be faxed or emailed will have a cover sheet stating the confidential nature of the information or a similar statement in the email. The following information will not be faxed:

1. Occurrence Reports

2. Employee Drug Screening Reports

3. Employee/patient/client HIV testing results

J. Information collected during performance improvement activities may be shared in statistical reporting formats.

K. Patient/client information boards (e.g., schedules, those needing aides/attendants, etc. will not be displayed in office common areas.

L. Agency will:

1. Avoid placing medical records in unattended areas accessible to unauthorized individuals.

2. Store medical records in a manner that minimizes the possibility of damage from fire and water.

3. Implement guidelines as to when release/removal of medical records is allowed (see Medical Record Information on Release and Removal policy).

4. Implement guidelines regarding copying the medical record which include:

   a. Which portions of the record may be copied and for what purposes;

   b. Staff accountability for protection of copies in their possession; and

   c. Control of the destruction of record copies.

5. Maintain confidentiality during and after normal business hours.

M. Agency will secure written contracts that include confidentiality clauses from but not limited to:

1. Contracted agents to complete the regulatory reporting requirements

2. Contracted billing companies who are bill via electronic claims

3. Business associates

N. Employee found to be in violation of this policy will be subject to discipline up to termination of employment.

II. Breach Notification for Unsecured Protected Health Information (PHI)

A. A breach occurs when protected health information is acquired, accessed, used, or disclosed in a way that compromises the protected health information.

B. Patient/client will notified within 60 calendar days from discovery when a breach of protected health information occurs. The breach notification must include:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

2. A description of the types of *unsecured* protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

3. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

4. A brief description of what the agency involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address

C. Agency must send written notification:

1. To patients/clients via first-class mail, at their last known address or electronically when patients/clients have agreed to this form of communication.

2. If patients/clients are deceased, notification should be mailed to patient's/client's next of kin or personal representatives.

3. In an emergency situation in which imminent misuse of the health information may occur, Agency may notify individuals by telephone or other means, in addition to providing written notice.

4. If written notice is impossible to provide due to incomplete or outdated contact information, a substitute form of notice must be provided. When there is insufficient contact information for fewer than ten (10) individuals, notice may be given by telephone, another type of written communication, or other means. When sufficient contact information is unavailable for ten (10) or more individuals, such notice shall:

   a. Be in the form of either a conspicuous posting for a period of 90 days on the home page of the Web site of the agency involved, or

   b. Conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and

   c. Include a toll-free telephone number that remains active for at least 90 days that individuals can use to learn whether their unsecured protected health information may be included in the breach.

D. Agency also has a duty to notify the media of a breach affecting more than five hundred (500) individuals residing in one State or jurisdiction. In this situation, agency must notify "prominent media outlets" serving the particular State or jurisdiction. Notice must be in written form and given no later than sixty (60) days after discovery of the breach.

E. The Secretary of HHS must also receive notice of breaches

1. When five hundred (500) or more patients/clients are involved, Agency must mail written notification to the Secretary at the same time as it is sent to the individuals affected.

2. For breaches involving fewer than five hundred (500) patients/clients, providers must maintain documentation of these breaches throughout the year. This documentation must be sent to the Secretary no later than sixty (60) days after the end of the calendar year.