RESPECT FOR PRIVACY, SECURITY, PROPERTY, AND THE RED FLAGS RULE

PURPOSE

To ensure the patient's/client's right to privacy and security, as well as respect for patient's/client's property, is observed and there is protection against identity theft.

POLICY

Agency will give the Notice of Privacy Practices to the Board of Directors, staff involved in patient/client care, potential employees, health care students, consultants and Business Associates which explains the patient's/client's rights regarding confidentiality, privacy, and security.

Agency will give and explain to the patient/client/caregiver the Notice of Privacy Practices regarding privacy rights as mandated by the Privacy Rules of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and its revisions, as applicable.

Agency will comply with the HIPAA Security Rules, effective April 21, 2005, (45 CFR Part 164), to protect all of the patients' electronic Protected Health Information (PHI).

If the Agency bills the patient/client for services and accepts credit cards or otherwise defers payments, it follows its established policies and procedures to protect against identity theft as mandated by the Federal Trade Commission's Red Flags Rules 16 CFR §681.2 and the Fair Credit Reporting Act as amended by the Fair and Accurate Credit Transactions Act of 2003.

The Board of Directors will be informed of and sign a "Conflict of Interest Statement."

The patient/client/caregiver will be informed on admission regarding confidentiality and the Agency's measures to protect against identity theft.

The patient's/client's property will be respected during the provision of patient/client care.

PROCEDURE

HIPAA Privacy Rules

A. Clinical

1. The Agency shall provide all current employees with training on the HIPAA Privacy Rule.

2. All new employees shall receive privacy training during their orientation.

3. If the Agency changes its policies and procedures, all employees shall receive retraining.

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

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

5. On admission, patient/client/caregivers will be informed both verbally and in writing regarding confidentiality, as well as access to, release of and the safeguarding of patient/client records as delineated in the Notice of Privacy Practices.

   5.1 This information includes:

   - Request to restrict use and disclosure of health information
   - Request to receive confidential communications
   - Request to access PHI
   - Request to amend PHI
   - Request for disclosure of PHI.

5.2 The need for Authorizations to release information to individuals not covered by HIPAA will be explained.

5.2.1 The patient/client will be instructed to contact the Privacy Officer.

5.3 The patient/client shall be assured that the Agency will:

- Restrict employees to access to the minimum amount of PHI necessary to do their job
- Disclose only the minimum amount of data necessary per the requested purpose
- Request only the minimum amount of PHI needed from other covered entities

5.4 The patient/client will be informed of the option to opt out of receiving fund-raising information per the Notice of Privcay Practices

5.5 The patient/client will be informed of the option to opt out of receiving marketing information per the Notice of Privacy Practices.

6. Agency staff will obtain a consent to obtain photographs of patient/client and/or patient/client wounds prior to taking the photograph.

B. Business

1. The Agency restricts the use and disclosure of certain types of information that could be advantageous to other businesses or harmful to the agency, its patients/clients or its employees.

2. Confidential business information is considered agency property.

3. Utilization of confidential information for personal gain is considered by the agency to be improper and/or unlawful.

4. Discussion of confidential information with family, friends or business and professional associates should be avoided.

5. Employees will be educated regarding confidentiality pertaining to use of electronic record/Point of Care device/laptop/personal digital assistants (PDAs)/USB flash drives/computers in the home, information kept in the car, discussions of one patient/client to another and other aspects of potential breech confidentiality. Employee education regarding confidentiality will include, as appropriate, the utilization of Smart Phones, Wireless Access Points (WAPs), Memory Cards, floppy disks; CDs, DVDs, backup media, Smart cards, and Remote Access Devices (including security hardware).

6. Employee data/information requested on hire and periodically, will be required and pertinent to the agency's business.

7. Employees/Board of Directors have a responsibility to have no conflicting interest when they represent Agency in negotiations or make recommendations about a third party. The employees/Board of Directors will work with patient/client, caregivers and other parties doing business with Agency on the basis of what is in Agency's best interest without showing favor or preference to third parties based on personal considerations.

8. An employee/Board of Director who deals with third parties on behalf of the agency or who makes recommendations or approves or rejects them shall not own any interest in or have any personal contact with the third party that could possibly influence the employee in regard to the best interest of the Agency.

9. An employee/Board of Directors shall not directly or indirectly seek or accept payments, loans, services, excessive entertainment, travel, gifts, or other reward from any individual or representative of any business or individual seeking to do business with the agency that might tend to influence the decision of the employee with respect to the agency's business.

C. Business Associates

1. The Agency's Business Associates shall have access to the minimum amount of patient/client PHI needed to accomplish the cited purpose. (See the Professional Services Contract.)

HIPAA Security Rules

1. The Agency shall appoint an Information Security Officer to oversee compliance with the HIPAA Security Rules.

   1.1 This individual may be the Privacy Officer.

2. The Agency shall provide security and awareness training to all of its employees, including management, upon hire and periodically thereafter.

3. The Agency shall perform an initial risk assessment for ePHI to ensure its security measures allow it to reasonably and appropriately comply with the HIPAA Security Rule.

   3.1 In deciding if its security measures are adequate, the Agency may consider the following:

   - Its size, complexity, and capabilities
   - Its technical infrastructure, hardware, and software security capabilities
   - The costs of the security measures
   - The probability and criticality of potential risks to electronic PHI

   3.2 The Agency shall perform follow-up ePHI risk assessments at periodic intervals including after any event that compromises the Agency's electronic security.

4. The Agency shall ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits.

5. The Agency shall protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI.

6. The Agency shall protect against any reasonably anticipated uses or disclosures of electronic PHI other than those that are permitted by the HIPAA Security Rule.

7. The Agency shall obtain assurances in a written contract from its Business Associate(s) that creates, receives, maintains, or transmits electronic PHI on its behalf that the Business Associate will safeguard the information.

8. The Agency shall ensure compliance with the HIPAA Security Rule by all of its employees, including management, and its Business Associate(s).

   8.1 The Agency shall institute sanctions against any employee as defined in its progressive discipline policy up to and including termination.

   8.2 The Agency shall terminate the contract with the Business Associate(s) if it determines there has been a violation to the HIPAA Security Rule.

9. The Agency shall maintain the policies and procedures implemented to comply with the HIPAA Security Rule in written or electronic form.

   9.1 The Agency shall document any action or activity taken and all risk assessments made as required by the HIPAA Security Rule.

   9.2 The Agency shall make documentation available to those responsible for implementing the procedures recorded and to appropriate regulatory entities.

9.3 The Agency shall review the documentation periodically and update it as needed in response to environmental or operational changes affecting the security of the patients' electronic PHI.

9.4 The Agency shall retain the required documentation for six years from its creation or the date when it was last in effect, whichever is later.

Red Flags Rules

1. Agency will determine if it is a "creditor" per the Red Flags Rules.

   1.1 Agency may be a "creditor" if it defers payments for goods and/or services.

2. Agency will determine if it offers or maintains "covered accounts," which are the extension of credit for goods or services involving a deferred payment.

   2.1 A "covered account" is one that is primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions.

   2.2 A "covered account" is any other account that the Agency offers or maintains for which there is a reasonably foreseeable risk to the patient/client or to the safety and soundness against identity theft.

3. Agency's Identity Theft Prevention Program (Program) includes, but is not limited to:

   3.1 Identifying Red Flags and risks to incorporate into the Program;

   3.2 Detecting Red Flags that have been used to perpetrate identity theft;

   3.3 Responding appropriately to Red Flags that have been detected to prevent and mitigate identity theft;

   3.4 Ensuring the Program is updated periodically to reflect changes in risks to the patient/client and to the Agency's safety and soundness;

3.5 Obtaining approval of the Program from the Board of Directors or Governing Body;

3.6 Involving the Board of Directors or Governing Body or designee from senior management in the oversight, development, implementation, and administration of the Program;

3.7 Appointing an oversight employee who is responsible for implementing, regularly administering, and annually reporting to the Board of Directors or Governing Body the Agency's compliance with the Red Flags Rule;

3.8 Training relevant staff to effectively implement the Program; and

3.9 Exercising appropriate and effective oversight of the contracts with patients/clients.

4. Red Flags are divided into categories for identification, prevention, and mitigation and include:

4.1 Alerts, notifications, or warnings from a consumer reporting agency

- A fraud or active duty alert is included with a consumer report;
- A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report;
- A consumer reporting agency provides a notice of address discrepancy;
- A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of a patient/client, such as:
  - A recent and significant increase in the volume of inquiries;

- An unusual number of recently established credit relationships;

- A material change in the use of credit, especially with respect to recently established credit relationships; or

- An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

4.2 Suspicious documents

- Documents provided for identification appear to have been altered or forged;

- The photograph or physical description on the identification is not consistent with the appearance of the patient/client presenting the identification;

- Other information on the identification is not consistent with information provided by the patient/client opening a new covered account;

- Other information on the identification is not consistent with readily accessible information that is on file with the Agency, such as a signature card or recent check; or

- An application appears to have been altered or forged or gives the appearance of having been destroyed and reassembled.

4.3 Suspicious personal identifying information

- Personal identifying information provided is inconsistent when compared against external information sources used by the Agency, such as:

  - The address does not match any address in the consumer report or

- The Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File;

- Personal identifying information provided by the patient/ client is not consistent with other personal identifying information provided previously such as SSN or date of birth;

- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the Agency, such as:

  - The address on the application is the same as that provided on a fraudulent application or

  - The phone number on an application is the same as that provided on a fraudulent application;

- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources, such as:

  - The address on an application is fictitious

  - The phone number is invalid or is associated with a pager or answering service;

- The SSN provided is the same as that submitted by other persons applying for services;

- The person applying fails to provide all required personal identifying information on an application or in response to notification the application is incomplete;

- Personal identifying information provided is not consistent with personal identifying information that is on file with the Agency; or

- If the Agency uses challenge questions and the individual cannot provide authenticating information beyond that which would be available from a wallet or consumer report.

4.4 Unusual use of, or suspicious activity related to, the covered account

- Patient/client fails to make the first payment or makes an initial payment but no subsequent payments or
- The Agency is notified the patient/client is not receiving its statements/invoices in the mail.

4.5 Notice from patients/clients, victims of identity theft, law enforcement authorities, or others regarding possible identity theft in connection with covered accounts held by the Agency.

- The Agency is notified per above that it has opened a fraudulent account for a person engaged in identity theft.

5. Agency will implement processes to detect Red Flags

5.1 Verify the identity of the patient/client applying for services and

5.2 Monitor transactions and verify the validity of change-of-address requests

6. Agency will respond to, and mitigate instances of, identity theft depending on the degree of risk posed by measures such as:

6.1 Monitoring covered accounts;

6.2 Changing passwords;

6.3 Contacting the patient/client;

6.4 Notifying law enforcement officials as appropriate; or

6.5 Determining that no response is warranted under the particular circumstances.

7. Agency will update the program as technology changes and/or identity thieves change tactics.

7.1 Agency will update program in conjunction with mergers, acquisitions, change in ownership, alliances, joint ventures, and arrangements with other service providers.