Purpose: To ensure that patient information is kept confidential and secure.

Policy: The Agency will protect the privacy of the patient by maintaining the security and safety of all patient information.

Security standards are established to ensure that patient-identifiable information remains confidential and protected from unauthorized disclosure, alteration, or destruction. The Health Insurance Portability Accountability Act of 1996 mandates the adoption of security standards for all healthcare facilities. Security includes the physical and electronic protection of the integrity, availability, and confidentiality of computer based information and the resources used to enter patient information. The security of the records includes the storing, processing and communication of all patient identifiable data.

The Agency will not disclose patient health information without authorization, except as described below.

Plan of Care/Treatment: The Agency will use patient health information for the plan of care/treatment; for example, information obtained by a nurse will be recorded in the record and used to determine the course of treatment. The nurse and other health care professionals will communicate with one another personally and through the case record to coordinate care provided.

Payment: The Agency will use patient health information for payment for services rendered. For example, the Agency may be required by insurance company to provide information regarding patient health care status so that the insurer will reimburse for the services provided. The Agency may also need to obtain prior approval from the insurer and may need to explain to the insurer the need for home care and the services that will be provided to patient.

Health Care Operation: The Agency will use health information for health care operations. For example, Agency therapist, nurses, field staff, supervisors and support staff may use information in the patient record to assess the care and outcomes of the patient case and others like it. This information will then be used in an effort to continually improve the quality and effectiveness of services we provide. Regulatory and
Notification: In an emergency, the Agency may use or disclose health information to notify or assist in notifying a family member, personal representative or another person responsible for patient care, of your location and general condition.

Workers’ Compensation: The Agency may disclose health information to the extent authorized by and to the extent necessary to comply with laws relating to workers’ compensation or other similar programs established by the law.

Public Health: As required by federal and state law, the Agency may disclose health information to public health or legal authorities charged with preventing or controlling disease, injury or disability.

Law Enforcement: As required by federal and state law, the Agency will notify authorities of alleged abuse/neglect; and risk or threat of harm to self or others. We may disclose health information for law enforcement purposes as required by law or in response to a valid subpoena.

Charges against the Agency: In the event a patient should file suit against the Agency, the Agency may disclose health information necessary to defend such action.

Duty to Warn: When a patient communicates to the Agency a serious threat of physical violence against himself, herself or a reasonably identifiable victim or victims, the Agency will notify either the threatened person(s) and/or law enforcement.

The Agency may also contact the patient about appointment reminders, treatment alternatives or for public relations activities.

In any other situation, the Agency will request written authorization before using or disclosing any identifiable health information about the patient. The patient can choose to sign such authorization to disclose information and can revoke that authorization to stop any future uses and disclosures.
Patient Notice/ Rights

Patients have the following rights with respect to their protected health information:

1. The patient may request in writing that the Agency not use or disclose information for treatment, payment or administration purposes or to persons involved in patient care except when specifically authorized, when required by law, or in emergency situations. The Agency will consider the patient request; however, the Agency is not legally required to accept it. The patient has the right to request that health information be communicated to in a confidential manner such as sending mail to an address other than patient home.

2. Within the limits of the statutes and regulations, the patients have the right to inspect and copy their protected health information. If you request copies, the Agency will charge you a reasonable amount, as allowed by statute. Patients may request a copy of their electronic medical record in an electronic form. The Agency will charge you a reasonable amount, as allowed by statute for providing a copy of the electronic medical record.

3. If the patient believes that information in the record is incorrect or if important information is missing, the patient has the right to submit a request to the Agency to amend the protected health information by correcting the existing information or adding the missing information.

4. The patient has the right to receive an accounting of disclosures of protected health information made by the Agency for certain reasons, including reason related to public purposes authorized by law and certain research. The request for an accounting must be made in writing to Administrator. The request should specify the time period for the accounting. Accounting request may not be made for periods of time in excess of six (6) years. The Agency would provide the first accounting request during any 12-month period without charge. Subsequent accounting request may be subject to a reasonable cost based fee.

5. When patients pay by cash they can instruct this agency not to share information about their treatment with their health plan/ insurance provider.

6. This agency will not disclose genetic information.
7. This agency will not use patient information for the purpose of fundraising or marketing. This agency will not sale patient health information.

Agency Responsibilities

1. The Agency is required by law to maintain the privacy of protected health information and to provide patients with notice of its legal duties and privacy practices with respect to protected health information.
2. The Agency is required to abide by the terms of this Notice of its duties and privacy practices. The Agency is required to abide by the terms of this Notice as may be amended from time to time.
3. The Agency reserves the right to change the terms of this Notice and to make the new Notice provisions effective for all protected health information that it maintains. Prior to making any significant changes in our policies, Agency will change its Notice and provide the patient with a copy. Patients can also request a copy of our Notice at any time.
4. It is the duty of this agency to notify the patient of a breach of their protected health information. This agency will notify the patient within 15 business days of discovery of any breach in the patients protected health information. Notification will occur regardless of whether the breach was accidental or if a business associate was the cause. A “breach” of PHI is any unauthorized access, use or disclosure of unsecured PHI, unless a risk assessment is performed that indicates there is a low probability that the PHI has been compromised. The risk assessment must be performed after both improper uses and disclosures, and include the nature and extent of the PHI involved, a list of unauthorized persons who used or received the PHI, if the PHI was in fact acquired or viewed, and the degree of mitigation. This agency and if any business associate was involved must consider all the following factors in assessing the probability of a breach:
   - the nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
   - the unauthorized person who used the protected health information or to whom the disclosure was made;
   - whether the protected health information was actually acquired or viewed; and
   - the extent to which the risk to the protected health information has been mitigated.
“Unsecured” protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology.

Procedure:

1. Other than described PHI is only released with the written consent of the patient/responsible party or under written legal directive. Only the Administrator, DON, Case Manager, or Office Manager may release protected health information.
2. Release only copies of the record. The organization retains all original records.
3. Staff members will view the clinical record on a “need to know” basis as determined by the Supervisor, and/or Administrator.
4. Patient information will only be utilized for the purpose of promoting patient care. Any other means requires express written consent.
5. Keep files in a secured area to control access. Non agency personnel such as repair persons will be accompanied by an agency staff member at all times.
6. Discuss patients in private with authorized persons only.
7. Protect written communication regarding patients from being viewed by unauthorized individuals, such as phone messages, communication boards, computer entered data, etc.
8. “Travel files” may be used by staff.
9. Only take the travel file for the particular patient into the home. Travel files that are not contained on the staff personnel (e.g. either in hand or tote bag) must be kept locked up and out of public view at all times.
10. All records will be maintained in a lockable storage area or interior locked room and maintained together.
11. In the event unsecured PHI is breached this agency will perform a PHI Breach Risk Assessment to determine whether or not the incident requires notification of the patient. If a business associate is involved they must participate in the Risk Assessment.
12. If the breach is determined to have no or low probability of risk to the patient then the patient will not be notified. Any other risk factor requires the agency to notify the patient in writing within 15 business days of the conclusion of the determination.

Refer to:
Appointment of Clinical Record Manager
PHI Breach Risk Assessment