SUBJECT: PRIVACY AND CONFIDENTIALITY OF INFORMATION

PURPOSE:

To effectively and efficiently preserve the privacy and confidentiality of patient, staff, and business entity information in compliance with applicable laws, regulations, and standards. The Home Health Agency secures and protects Protected Health Information (PHI) and Electronic Protected Health Information (EPHI).

DEFINITIONS:

- Privacy: The patient has the right to a confidential patient record. An individual's right to limit disclosure of personal information.

- Confidentiality: The safekeeping of data/information so as to restrict access to individuals who have need, reason, and permission for such access.

- Protected Health Information: Health information that contains information such that an individual person can be identified as the subject of that information.

Examples of a non-covered entity who require a Business Associate Agreement on file at the Home Health Agency (as defined by HIPPA) include but are not limited to:
A CPA firm whose accounting services to a health care provider involves access to protected health information.
An attorney whose legal services to a health plan involve access to protected health information.
A consultant that has access to protected health information.
An independent medical transcriptionist that provides transcription services to a physician.

POLICY:

- Confidentiality of data and information within the Agency applies across all systems and automated, paper and verbal communications, as well as to clinical/service, financial and business records, and employee-specific information.

- All employees receive instructions about the Agency's Privacy and Confidentiality of Information policy and procedure during orientation and whenever new/updated information becomes available.

- Significant changes to the Agency's Privacy and Confidentiality of Information policy and procedure are communicated to staff members, including contracted personnel, in verbal and written formats. These formats include in-service programs, staff meetings, memos, e-mails, etc. Receipt of the information by employees is documented by employees' signatures (may include electronic signatures) and retained by the Agency.

- All Agency staff members are required to adhere to the Agency's Privacy and Confidentiality of Information policy and procedure. Failure to adhere to this policy and procedure will result in disciplinary action up to and including termination.

- All patient personal and health information and billing data is considered confidential and will be disclosed at the direction of Administration only when appropriately authorized to do so by the patient or his/her legal representative, pursuant to a subpoena with appropriate documentation, or on a "need to know" basis as necessary to carry out the day to day business activities: Participant, Legal Guardian, MPOA, Provider/staff caring for patient, and any agent of the Department of Health or designee may access PHI without permission.

- Patient information designated as "sensitive" i.e. psychotherapy notes, HIV/AIDS diagnosis, will be disclosed at the direction of Administration only when appropriately authorized to do so by the patient or his/her legal representative, pursuant to a subpoena with appropriate documentation, or when required to provide care, treatment, or services.

- All employee personal data, personnel records, work related information and pay records are considered confidential to be disclosed at the direction of Administration only when authorized to do so by the employee or employee's legal representative, when required to do so by law, or on a "need to know" basis as necessary to carry out day-to-day business activities.

- All Agency business records and/or dealings are considered confidential to be disclosed only when authorized to do so by Administration, pursuant to a subpoena with appropriate documentation, or on a "need to know" basis as necessary to carry out day-to-day business activities.

- Home care medical records, personnel records, computerized data systems, and billing records are protected from loss, alteration, unauthorized use or damage, and stored in a locked, secure location.

- Computer files, including OASIS data encoding and transmission files, are password protected against unauthorized use, alteration, or damage.

- Passwords are not to be shared and are not to be displayed. Passwords are changed periodically at the discretion of Administration.

- Patient, employee and company information is de-identified during performance improvement activities, in memos, and when included in meeting minutes.

- Patient information shall not be displayed in areas accessible to the public and/or unauthorized personnel.

- All staff shall limit discussion of patient care, treatment and/or services to appropriate personnel within the Agency and/or pertinent individuals under contract who have

legitimate needs for accessibility of the information for delivery of care, treatment and/or services, effective functioning of the organization, research and/or education.

- Cell phones may be used in a patient's home to communicate information about that particular patient to appropriate individuals i.e. physicians, Agency staff. Cell phones are not to be used in the patient's home to communicate information about other patients, for personal communications, and/or in public areas, including but not limited to patient care facilities.

- Telephone communication regarding patient, employee and/or company information is to be conducted in a manner that protects the privacy of the information to the extent possible and is not to be conducted in public places.

- The Agency accepts authorizations, physician orders, laboratory reports, etc. via facsimile (fax) transmission and/or via telephone.

- When transmitting a fax, the staff member is to verify that the fax recipient is available before sending the fax and should verify that the fax was received. List the fax cover letter spelling out the following information is protected by HIPPA and is confidential.

- Incoming facsimile information is to be removed from the machine immediately, the correct number of pages verified, and the information is to be delivered to the recipient.

- Release of information forms shall specify the information the patient or his/her legal representative is authorizing the Agency to disclose.

PROCEDURE:

- The Administrator will review all requests for information to determine whether or not the request will be honored.

- Access to information and records, including computer access, is determined by the requesting individual's "need to know" as follows:

- Professional and field personnel directly involved in providing care, treatment and/or services to the patient are permitted access to the patient's medical records.

- Operational and professional personnel of the Agency, who require access to patient records, employee records or Agency records in order to accomplish their day-to-day tasks, are permitted access to needed records as described within this policy.

- Telephone requests for employee or patient information are directed to the Administrator.

- Requests for disclosure of patient information to reimbursement organizations, healthcare organizations, physicians, and licensing and/or accrediting agencies require a completed and signed consent form and are referred to the Administrator.

- Agency leadership and clinical personnel directly involved in providing care, treatment and/or services to the patient are authorized to enter information into and to review patient records. Other Agency personnel authorized to enter information into and/or review patient records are those whose job responsibilities include these tasks or those authorized by the Administrator or Clinical Manager.

- Consents or Release of Information Signatures:

- Must be the original, legible, legal signature of the patient or employee; or,

- May be the original, legible, legal signature of the legal representative if the subject has a court appointed guardian; or,

- May be the original, legible, legal signature of a legally authorized representative of the patient or employee; or,

- May be the original, legible, legal signature of a family member if the patient is unable to sign. If signed by a family member, the signature should be witnessed and the reason for the patient's inability to sign documented.

- If the validity of a signature is questioned, the Agency has the right to require a notarized signature.

Safeguarding of Records:

- Original paper or computer patient medical records, personnel files, payroll records and billing records shall be filed and shall not be removed from the site of origin except pursuant to subpoenas with appropriate documentation, or for transfer to and from storage facilities or other authorized sites as needed to accomplish the day-to-day business of the Agency upon direction of Administration.

- Whenever records are transferred from the site of origin, the records must be safeguarded from public view at all times.

- Records should not be left in unattended areas accessible to unauthorized individuals.

- Records shall be stored in a manner that prevents loss, destruction of, or tampering with information.

- Back-up copies of computer records shall be stored and safeguarded in a manner to maintain the integrity of the system.

- Records may be photocopied by authorized employees as necessary to accomplish the day-to-day business of the Agency. Clerical and professional personnel may copy documents when authorized to do so as outlined below:

Document(s)	Authority
Medical Records, including OASIS data, or parts thereof	President, Administrator, Clinical Director/DON, Clinical Personnel, and others as designated by Administration
Personnel Records, or parts thereof	President, Administrator, Clinical Director/DON, and others as designated by Administration
Billing Records, including OASIS data, or parts thereof	President, Administrator, Billing Department, others as designated by Administration
Payroll Records	President, Administrator, and others as designated by Administration

- Relevant copies of the patient's medical record may be left in the patient's home as is necessary to assist the home healthcare staff in providing care, treatment and/or services to the patient.

- All copies of records, except those left in the patient's home for the express purpose of education and/or for reference, shall be returned to the Agency office and destroyed by shredding.

Record Retention

- All patient records shall be retained for a minimum of five (5) years from the date of the most recent discharge of the patient, five (5) years after the month the cost report to which the records apply is filed with the intermediary unless State law stipulates a longer time period.

- Records of minor patients or patients with guardians shall be retained until at least one (1) year following the patient's eighteenth birthday, or according to State laws and regulations.

- Final validation reports from submission of OASIS records and OBQI/IM reports shall be retained for a period of twelve (12) months until the new expected OBQI/IM reports are received.

- In the event the Agency should cease operations, the Administration shall retain the records in a secure location.

- Any records of cases involved in litigation shall be retained until the case is concluded, even if this is beyond the time period prescribed by law.

- Orientation and Education of Staff, members of the Governing body

- Review of the Agency's confidentiality policies and procedures.

- Guidelines for photocopying records.

- Guidelines for prevention of unauthorized disclosure of patient, employee and company information; and,

- The signing of a confidentiality statement that becomes a permanent part of each employee's and each member of the Governing body. The signed confidentiality statement is filed in each individual's respective personnel file.