## Purpose

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

## Definition

I. The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patient's rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

II. The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

III. The HIPAA Breach Notification Rule requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third-party service providers, pursuant to section 13407 of the HITECH Act.



## Policy

I. The Hospice will give the Notice of Privacy Practices to the Governing Body, all staff involved in patient care, potential employees, health care students, consultants and Business Associates which explains the patient's rights regarding confidentiality, privacy, and security.

II. The Hospice will give and explain to the patient and/or 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.

III. The Hospice will comply with the HIPAA Security Rules, to include and protect all of the patients' electronic Protected Health Information (PHI).

IV. The Hospice and any agent acting on behalf of the Hospice in accordance with a written contract must ensure the confidentiality of all patient identifiable information contained in the clinical record, and may not release patient identifiable information to the public.

V. The Governing Body members will be informed of and sign a "Confidentiality/Conflict of Interest Disclosure Statement."

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

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

**Procedure**

I. HIPAA Privacy Rules

A. Clinical

1. The Hospice will provide all current employees with training on the HIPAA Privacy Rule, including Privacy, Security, and Breach Notification.
2. All new employees will receive privacy training during their orientation.
3. If the Hospice changes its policies and procedures, all employees will receive retraining.
4. All privacy orientation and retraining will be documented in the employees' personnel files.
    a. The Privacy Officer will maintain a record of privacy, security, and breach notification training given to the employees as defined in the HIPAA Privacy, Security, and Breach Notification Rules.
5. On admission, the patient and/or caregiver will be informed both verbally and in writing regarding confidentiality, as well as access to, release of and the safeguarding of patient records as delineated in the Notice of Privacy Practices.
    a. This information includes, but not limited to:
        (1) Request to restrict use and disclosure of health information;
        (2) Request to receive confidential communications;
        (3) Request to access PHI;
        (4) Request to amend PHI;
        (5) Request for disclosure of PHI; and
        (6) Right to be notified following a breach of his or her unsecured PHI.
    b. The need for Authorizations to release information to individuals not covered by HIPAA will be explained.
    c. The patient will be instructed to contact the Privacy Officer.

d. The patient will be assured that the Hospice will:

(1) Restrict employees to access to the minimum amount of PHI necessary to do their job;

(2) Disclose only the minimum amount of data necessary per the requested purpose; and

(3) Request only the minimum amount of PHI needed from other covered entities.

e. The patient will be informed of the option to opt out of receiving fund-raising information per the Notice of Privacy Practices.

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

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

B. Business

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

2. Confidential business information is considered the Hospice's property.

3. Utilization of confidential information for personal gain is considered by the Hospice 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 records, Point of Care devices, computers, electronic devices and media, information kept in the car, discussions of one patient to another and other aspects of potential breech confidentiality.

6. Employee education regarding confidentiality will include, as appropriate, the utilization of Smart Phones, Wireless Access Points (WAPs), Memory Cards, disks, CDs, DVDs, backup media, Smart Cards, and Remote Access Devices (including security hardware).

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

8. Employees and Governing Body have a responsibility to have no conflicting interest when they represent the Hospice in negotiations or make recommendations about a third party. The employees and Governing Body members will work with patients, caregivers, and other

parties doing business with the Hospice on the basis of what is in Hospice's best interest without showing favor or preference to third parties based on personal considerations.

9. An employee or Governing Body member who deals with third parties on behalf of the Hospice or who makes recommendations or approves or rejects them will 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 Hospice.

10. An employee or Governing Body member will 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 Hospice that might tend to influence the decision of the employee with respect to the Hospice's business.

C. Business Associates

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

II. HIPAA Security Rules

A. The Hospice will appoint an Information Security Officer to oversee compliance with the HIPAA Security Rules. This individual may be the Privacy Officer.

B. The Hospice will provide security and awareness training to all of its employees, including management, upon hire and periodically thereafter.

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

1. In deciding if its security measures are adequate, the Hospice may consider the following:

a. Its size, complexity, and capabilities;

b. Its technical infrastructure, hardware, and software security capabilities;

c. The costs of the security measures; and

d. The probability and criticality of potential risks to electronic PHI.

2. The Hospice will perform follow-up ePHI risk assessments at periodic intervals including after any event that compromises the Hospice's electronic security.

D. The Hospice will ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits.

E. The Hospice will protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI.

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

G. The Hospice will 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.

H. The Hospice will ensure compliance with the HIPAA Security Rule by all of its employees, including management, and its Business Associate(s).

1. The Hospice will institute sanctions against any employee as defined in its progressive discipline policy up to and including termination.

2. The Hospice will terminate the contract with the Business Associate(s) if it determines there has been a violation to the HIPAA Security Rule.

I. The Hospice will maintain the policies and procedures implemented to comply with the HIPAA Security Rule in written or electronic form.

1. The Hospice will document any action or activity taken and all risk assessments made as required by the HIPAA Security Rule.

2. The Hospice will make documentation available to those responsible for implementing the procedures recorded and to appropriate regulatory entities.

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

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

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

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

B. The patient will be notified within 60 calendar days from discovery when a breach of PHI 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 PHI 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 Hospice 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 will include a toll-free telephone number, an e-mail address, Web site, or postal address.

C. The Hospice must send written notification:

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

2. If patients are deceased, notification should be mailed to the patients' next of kin or personal representatives.

3. In an emergency situation in which imminent misuse of the health information may occur, the Hospice 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 10 individuals, notice may be given by telephone, another type of written communication, or other means. When sufficient contact information is unavailable for 10 or more individuals, such notice will:

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

E. The Secretary of Health and Human Services must also receive notice of breaches.

1. When 500 or more patients are involved, the Hospice 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 500 patients, providers must maintain documentation of these breaches throughout the year. This documentation must be sent to the Secretary no later than 60 days after the end of the calendar year.