Contact us at (903) 295 -1680 for more information. Effective May 22, 2025.

12.4 Privacy of Protected Health Information

Purpose: To comply with the Privacy Rule is located at 45 CFR Part 160 and Subparts A and E of Part 164 U.S. Department of Health and Human Services.

Policy:

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as "protected 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 protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization.

The Rule also gives individuals rights over their protected health information, including the right to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third party an electronic copy of their protected health information in an electronic health record, and to request corrections.

It is the policy of Heart'sWay Hospice to preserve and protect the rights of patients and families to control access to protected health information in accordance with state law and federal regulations. Protected Health Information (PHI) is individually identifiable information related to the provision of or payment for health care in written, electronic or verbal form.

Records Storage: Written PHI will be stored in private areas of the office. The office is to be locked whenever it is not occupied. Chart storage is no longer be needed – we have completed the transition to 100% electronic charts.

Public Office Areas: The public areas of the office are the hallways, conference room, restrooms and coffee area. Protected health information should never be kept in these areas when it is not constantly attended. Particular attention should be paid to removing PHI from the conference room after meetings.

Vehicles and Homes: The majority of PHI carried in the field is safe and secure on laptop and tablet computers. See our security policies on controlling access to information on these devices. From time to time, paper documentation that needs to be protected may be transported in the field. This needs to be kept out of sight in a locked vehicle when not being used and moved to a secure location ASAP while not in the staff person's possession.

Awareness of privacy principles is the most important thing in controlling verbal communication of PHI. Health information required for treatment, payment or operations may be communicated freely both inside that Agency and outside the Agency in accordance with the minimum necessary rule. Discretion needs to be used in communicating this information in public or semi-public areas.

Be aware of requests for restrictions and requests for confidential communications and honor requests that have been approved in verbal, as well as written, communications. Consult the Privacy Officer if you have any questions regarding this.

Particular attention needs to be paid to disclosing PHI over the telephone. Be aware of the caller's identity, their standing with the patient/family and with our Agency and their specific needs for

information whenever anyone requests PHI over the phone. Be aware of requests for restrictions and requests for confidential communications as above. Our policies require that some requests need to be made in writing. Remember the caller of the appropriate policy as necessary.

12.4.1 Privacy Officer

Purpose: The Executive Director will appoint a Privacy Officer who is responsible for overseeing the development, implementation, maintenance of, and adherence to privacy policies and procedures regarding the safe use and handling of protected health information (PHI) in compliance with federal and state HIPAA regulations.

Policy:

The Privacy Officer will be:

1. Responsibility to oversee all activities related to the implementation of and adherence to the organization's privacy practices, and to ensure operational procedures follow relevant privacy laws.
2. Monitors employees and systems about how information is collected, used, and disclosed and access to identifying information.
3. Serve as the designated contact person in Heart'sWay Hospice's Notice of Privacy Practices to receive questions and complaints related to the protection of health information
4. Ensure that Notice of Privacy Practices, consent and authorization forms, business associate contracts and privacy policies and procedures comply with the HIPAA Privacy Rule
5. Review, respond to and document requests for restrictions, requests for disclosures, requests to amend and requests for an accounting for PHI
6. Coordinate and/or conduct privacy training and maintain privacy records in accordance with the Agency's policies and procedures
7. Serve as internal and external liaison and resource between the Agency, its employees and outside entities including vendors, oversight agencies, accrediting bodies and the Office of Civil Rights
8. Investigate suspected noncompliance with the Agency's privacy practices and report noncompliance to the Executive Director. Design and implement remedial measures to prevent reoccurrence.

12.4.2 Staff Education and Training

Purpose:

(§164.530(b)(1) HIPAA Privacy Rule and (§164.308(a)(5) HIPAA Security Rule discuss the scope and depth of the training required

1. **Privacy Rule**: Provides federal standards to safeguard the privacy of personal health information, including patients' rights to examine and obtain a copy of their health records and request corrections.
2. **Security Rule**: Covers electronic protected health information (e-PHI) and has detailed requirements regarding privacy and security.

Hipaa Privacy Rule's Administrative Requirements standards include:

"*Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate." (45 CFR § 160.103)***.**

"A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity."

HIPAA Privacy Rule training:

1. Implement a security awareness and training program for all members of its workforce including management, all staff members, volunteers, and business associates.
2. The Agency provides training for all current and new staff members and volunteers who have access to protected health information.
3. All members of the Agency's workforce, including volunteers who were employed prior to April 14, 2003
4. All new employees and volunteers as a component of their orientation to the Agency after April 14, 2003
5. All members of the Agency's workforce, including volunteers, will receive training annually, if privacy policies and procedures change, if risk assessment identifies areas that impact compliance and as necessary.
6. Documentation of privacy training is maintained by the Privacy Officer.

HIPAA Security Training: Section §164.306 contains the General Requirements for the HIPAA Security Rule, which states covered entities and business associates must protect against any reasonably anticipated uses or disclosures not permitted under the Privacy Rule.

1. Implement a security awareness and training program for all members of its workforce including management, all staff members, volunteers, and business associates.
2. Must include:
    a) Periodic security updates.
    b) Procedures for monitoring login attempts and reporting discrepancies.
    c) Procedures for creating, changing, and safeguarding passwords.
    d) Procedures for creating, changing and safeguarding passwords.

12.4.3 Business Associates

Definition: According to the Department of Health and Human Services (HHS), a BA is a person or entity, other than a member of the workforce of a covered entity who performs functions or activities on behalf of, or provides certain services to, a covered entity that involves access by the business associate to PHI. A BA also is a subcontractor that creates, receives, maintains, or transmits PHI on behalf of another BA. In other words, if a third-party organization could potentially have access to PHI while carrying out their assigned tasks, they are a business associate. Under HIPAA there are two different entities accountable for protecting PHI:

1. Covered Entities-Most of the covered entities are businesses that interact directly with patients, such as hospitals, doctors' offices, and clinics, or that have access to their data, like insurance providers
2. Business Associates- most don't interact with patients; they may administer or have access to their medical records. Examples of business associates may include:
    - Accrediting bodies
    - Answering services
    - Clinical software vendors
    - Cleaning services
    - Consultants
    - Attorneys

Purpose: The business associates of Heart'sWay Hospice are required to provide satisfactory **assurance** that they will maintain the confidentiality of the protected health information of our patients and only use and disclose it for the purposes for which it was provided. Since both covered entities, and their business associates (BA) are responsible for keeping PHI safe, it's in their best interests to have an BAA in place and to maintain a thorough understanding of their relationship and how they expect one another to secure patient, client, or employee data. All covered entities are required by the HIPAA Privacy Rule to have signed BAAs with any BAs they hire who may have access to PHI.

Procedure:

1. Existing and new relationships with entities providing services on our behalf are reviewed to determine if the relationship will require the use and/or disclosure of protected health information and therefore be classified as a business **associate**.

2. Business associates are required to sign a written contract or contract amendment (Business Associate Contract) that outlines the party's responsibilities in relation to PHI.

    a) BAAs explains the authorized and unauthorized uses of PHI between two HIPAA-responsible businesses.

    b) To maintain the confidentiality, integrity, and availability of electronic protected health information (ePHI), the contract shall require that the BA establish the

proper administrative, technical, and physical safeguards in accordance with the Security Rule.

c) The contracts can also be designed to include information about relationships between a covered entity and a BA, as well as relationships between two BAs.

d) The consequences of disobeying HIPAA regulations should also be explained to a BA. Regulators have the authority to penalize BAs directly for HIPAA violations.

e) The contract must include the criteria of 45 CFR 164.504(e).

- Determine what PHI the BA will access
- Require that the BA will use proper security measures to protect PHI
- Provide that the BA will not disclose PHI unless permitted by the agreement
- Require and track necessary HIPAA Training for employees
- Define procedures in the event of a data breach
- Contain necessity subcontractor compliance
- Detailed conditions for the termination of the agreement
- Describe the process of destruction or return of PHI

3. The Agency's Contract Coordinator (Assistant Executive Director) is responsible for ensuring that contracts and amendments comply with this policy.
4. The Privacy Officer will ensure that any complaints regarding privacy violations on the part of the business associate are reviewed and will make recommendations to the Executive Director regarding remedial measures to prevent recurrence as necessary and appropriate.

12.4.4 Consent to Use and Disclose Protected Health Information

In accordance with the Privacy Rule, the Agency may request, use and disclose PHI required for treatment, payment or operations subject to the minimum necessary rule without any additional consent or authorizations. However, the Agency's policy is to request or require three consents upon admission:

1. A Financial Authorization Form consenting to the Agency to release medical records required by insurers and/or their fiscal intermediaries, or substantiating payment for, services rendered to patients insured by Medicare, Medicaid or third-party payers.
2. A Release of Medical Information form consenting for us to request medical information from hospitals, physicians, or other health care providers.
3. A Consent to Provide Caregiver, Family and Bereavement Support form consenting to disclosure of PHI to provide caregiver, family and bereavement support to family, friends and caregivers. The patient or personal representative also has an opportunity on this form to request that we not disclose PHI to specific individuals unless otherwise permitted or required by law. Review of and compliance with such requests will be per the procedures listed under "Request for Restrictions".

12.4.5 Minimum Necessary Rule

Heart'sWay Hospice's employees, volunteers and business associates will use, disclose or request the minimum amount of protected health information necessary to perform their job functions.

Review of the roles within the EMR system will occur on employment and periodically to ensure that minimum necessary access is assigned.

Procedure:

1. The Agency identifies the employees, volunteers and business associates who need access to protected health information according to the categories of uses for treatment, payment or health care operations.
2. The Agency identifies the type and minimum amount of protected health information needed by employees, volunteers and business associates to perform their jobs.
3. The Agency determines the circumstances under which employees, volunteers and business associates may use, disclose or request protected health information.
4. All members of the interdisciplinary team, student interns and others who provide and coordinate treatment for patients and caregivers have access to the patient's entire medical record.
5. The Agency reviews non-routine requests for disclosures of health information that are not related to treatment on a case-by-case basis unless the patient has authorized the request. This is the responsibility of the Privacy Officer.
6. Non-routine requests for disclosure are forwarded to the Privacy Officer to determine if the amount of health information is the minimum necessary to achieve the purpose of the disclosure according to established criteria.
7. The Agency relies on representations that the information requested is the minimum amount necessary if the request is from a public official, a health care provider, a health plan or a professional providing services as a business associate.
8. When necessary and appropriate, the Privacy Officer will speak with a representative from the entity making a request for clarification and/or modifications.
9. The Agency does not disclose an individual's entire medical record in fulfillment of any request not related to treatment for any reason unless a justification for such a disclosure is documented.

12.4.6 Authorizations

Authorizations are required for the use and disclosure of protected health information for purposes other than treatment, payment and health care operations or as otherwise provided by law. Protected health information procured under the terms of these documents will only be used or disclosed as specified in the Agency's Notice of Privacy Practices and in this policy. Disclosures of PHI pursuant to a valid authorization are exempted from the Minimum Necessary Rule.

An authorization must specify several elements, including a description of the protected health information to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, and, in some

cases, the purpose for which the information may be used or disclosed. With limited exceptions, covered entities may not condition treatment or coverage on the individual providing an authorization.

The Agency uses a separate authorization form in the following circumstances:

1. For a patient to request that their protected health information be used or disclosed for reasons other than treatment, payment or operations or as otherwise authorized under a valid consent or authorization.
2. When the Agency asks the patient for permission to use their protected health information for its own purposes other than treatment, payment or operations or as otherwise authorized under a valid consent or authorization.
3. Whenever release of the entire medical record is requested.

Procedure:

1. When authorization is needed or requested, the patient or his/her representative is provided with a copy of the authorization form and is asked to sign it.
2. Signing the authorization form is voluntary.
3. The HIPAA Privacy Rule expressly requires authorization for uses or disclosures of protected health information for ALL marketing communications, except in two circumstances:
   a) When communication occurs in a face-to-face encounter between the covered entity and the individual; or
   b) Communication involves a promotional gift of nominal value.

   If the marketing communication involves direct or indirect remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved.
4. A copy of the authorization is provided to the individual who signs it.
5. The authorization may be revoked (in writing) by the patient/representative at any time.
6. The permissions granted in the authorization may not be acted upon if it has been revoked or if it has expired.
7. The authorization is documented, filed in the clinical record and retained for a period of six years after it was created or expired, whichever date is later.

12.4.7 Privacy Rights

Purpose: § 164.520 Code of Federal Regulations

1. ***Right to notice.*** Except as provided by paragraph (a)(3) or (4) of this section, an individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

(2) ***Notice requirements for covered entities creating or maintaining records subject to 42 U.S.C. 290dd-2.*** As provided in 42 CFR 2.22, an individual who is the subject of records protected under 42 CFR part 2 has a right to adequate notice of the uses and

disclosures of such records, and of the individual's rights and the covered entity's legal duties with respect to such records.

Patients cared for by Heart'sWay Hospice have the following privacy rights:

- To receive a paper copy of the organization's Notice of Privacy Practices
- To request restrictions on the uses and disclosures of health information
- To request to receive confidential communications
- Patients have the right to access and obtain copies of their protected health information in any form requested in a timeframe by responding to request in 15 days. A fifteen-day extension may be requested.
- To access their protected health information for inspection and/or copying
- To amend their health care information
- To request an accounting of disclosures of health information

The following policies detail the specific requirements for each of these rights and provide procedures for implementation.

12.4.7.1 Notice of Privacy Practices

The Agency's Notice of Privacy Practices (Notice) will be given to all patients or their designated representatives upon admission to the Agency. The staff, business associates and the public will be informed of the Agency's privacy practices.

Procedure:

1. The privacy practices of Heart'sWay Hospice are described in the Notice of Privacy Practices.
2. The Notice of Privacy Practices will be given to all patients/designated representatives upon admission to the Agency. This is the responsibility of the admitting professional.
3. The admitting professional will make a good faith effort to obtain a written acknowledgement or the patient's receipt of the Notice or document the reason that an acknowledgement was not obtained. This information will be filed in the patient's clinical record.
4. All staff and volunteers will receive training in the Agency's privacy practices.
5. The Notice of Privacy Practices will also be posted on the Agency's web site.
6. All business associates will receive a copy of the Notice of Privacy Practices.
7. The Notice of Privacy Practices will be revised as necessary. Prior to the effective date of each revision, all patients, employees and business associates will receive a copy of the revision.
8. The Privacy Officer will maintain a copy of each version of the Notice for the latter of six years from the date of its creation or when it was last in effect.
9. All employees and business associates of the Agency are required to adhere to the privacy practices as detailed in the Notice of Privacy Practices.

12.4.7.2 Requests for Restrictions

Patients or their representatives have the right to request restrictions on how their protected health information is used and/or disclosed.

Procedure:

1. Patients are informed of their right to request restrictions on the use and disclosure of their protected health information in the Agency's Notice of Privacy Practices.
2. Patients are verbally informed of this right during each admission. They are given the opportunity to identify any individuals that should be restricted in the Consent to Provide Caregiver, Family and Bereavement Support form. This form is filed in the privacy section in each patient's chart and guides us in deciding whether to restrict the release of PHI to any individual under normal circumstances.
3. Requests to release or restrict the release of PHI under abnormal circumstances should be forwarded to the Privacy Officer for a determination.
4. Hospice employees may not grant or deny a patient's request for such restrictions without prior authorization from the Privacy Officer or designee.
5. Heart'sWay Hospice will agree to a patient's request for restrictions on the use and disclosure of their health information if it is reasonable and, in the patient's, best interests.

   The Agency will always agree to a patient's request for restrictions on the use and disclosure of their health information if the disclosure is to a health plan for purposes of carrying out healthcare operations or payment (and not for treatment purposes), except as required by law.

When a request for restriction(s) is accepted:

1. The patient will be informed of any potential consequences of the restriction.
2. A notation will be made in the patient's clinical record.
3. The Agency will not use or disclose protected health information inconsistent with the agreed restriction, nor will its business associates.
4. The patient will be informed that Heart'sWay Hospice is not required to comply with the agreed upon restrictions in emergency treatment situations.
5. If the agreed upon restriction hampers treatment, the Agency will ask the patient to modify or revoke the restriction and get a written agreement to the modification or revocation or document an oral agreement.
6. The use and/or disclosure of protected health information will be consistent with the status of the restriction in effect on the date it is used or disclosed.
7. Written documentation of any restrictions on PHI will be maintained for six years from the date of its creation or the date when it was last in effect, whichever is later.

A request for restrictions) s may be denied:

1. If the restriction would negatively affect the patient's care
2. If the restriction is not in the patient's best medical interest
3. The request is unreasonable and would make the provision of care impossible

When a request is denied:

1. The patient will be provided with an explanation of the reasons for denial.
2. If a patient will be given the opportunity to discuss his or her privacy concerns if desired.

3. Efforts will be made to assist the patient in modifying the request for restrictions to accommodate their concerns and obtain agreement by the Agency.

12.4.7.3 Requests for Confidential Communications

Patients have the right to request restrictions on how and where their protected health information is communicated.

Procedure:

1. Heart'sWay Hospice requires that patients who desire their health information be communicated in an alternative manner or location than the hospice would otherwise use, to specify the alternative location or other method of contact.
2. The Agency does not require that the patient provide a reason for the request.
3. The Agency does not refuse to accommodate the request unless it imposes an unreasonable administrative burden or is contrary to the Plan of Care.
4. The patient may request confidential communication at the time of admission or at any time during their care.
5. The request may be made to the admissions staff or to any member of the Interdisciplinary Team.
6. When a request is made, either formally or informally, the person receiving the request will document it in writing.
7. Requests will be forwarded to the Privacy Officer or designee for review and further action.
8. Written documentation of the patient's request, if granted, will be placed in the patient's clinical record.
9. If the Agency **can** accommodate the patient's request, all members of the Interdisciplinary Team who provide care to the patient will be provided with information regarding the communication requirements and will be expected to adhere to them.

12.4.7.4 Requests for Access for Inspection and/or Copying

Except in certain circumstances patients and/or primary caregiver/legal representative have the right to access and obtain copies of their protected health information in a "designated record set". The designated record set is that group of records maintained by or for the covered entity that is used, in whole or part, to make decisions about individuals, or that is a provider's medical and billing records.
The information will be provided in any form requested, in a timeframe by responding to requests in 15 days. A fifteen-day extension may be requested.
Exceptions to the rule are psychotherapy notes, information compiled for legal proceedings, lab results to which the CLIA Act prohibits access, information held by certain research laboratories, and the use and disclosure of substance use disorder patient records which are maintained in connection with the performance of any part 2 program.

Procedure:

1. Requests for access to health information may be verbal.
2. These requests should be forwarded to the Privacy Officer for review and further action.

3. These requests will be made within three working days.
4. If the agency denies the request the individual can request a review by the agency's Ethics committee for reconsideration. Results of the Ethics Committee decision will be provided to the individual in writing.

Other Designated Representatives

1. Heart'sWay Hospice requires and informs individuals that requests for access to personal health information must be made in writing.
2. Requests will be forwarded to the Privacy Officer or designee for review and further action.
3. HeartsWay Hospice maintains health information that may be subject to requests for access for a period of six years from the date it was created or was last in effect whichever comes later.
4. The agency maintains a record of the person or office responsible for processing and receiving requests for access for a period of six years

When a request for access is accepted (in whole or in part)

1. The individual is notified of the decision and may choose to inspect the health information, copy it, or both, in the form or format requested. If the protected health information is not readily producible in the form and format requested, a readable hardcopy form or other format as agreed upon will be provided.

2. If the requested PHI is maintained electronically in one or more designated record sets, the protected health information must be provided to the individual in the electronic form or format requested by the individual. If the requested form or format is not readily producible, the Agency must offer an alternate readable electronic format. If the individual does not agree to the alternative format, a hard copy may be provided to fulfill the request for access.

3. The Agency and the individual will arrange a mutually convenient time and place for the individual to inspect and/or obtain a copy of the requested information.

4. The Agency must mail a copy of the requested health information if the individual prefers this method of obtaining a copy.

5. The Agency will transmit a copy of the PHI directly to another person provided that the request to do so is made in writing, signed by the individual and includes clear identification of the designated person and where to send the protected health information.

Fees charged by Heart'sWay Hospice for access to health information

1. The Agency may require payment in advance for actual postage due and reasonable copying charges not to exceed $1.00 for the first page and $0.15 for each page thereafter.

2. No fee is charged for retrieving or handling the requested information or for processing the individual's request for access to their health information.

3. If a summary of the information is also requested, the Agency may charge a reasonable, **cost-based** fee for reviewing and summarizing the information.

12.4.7.5 Requests to Amend

Patients or their personal representatives have the right to request amendment of their health information.

Procedure:

1. Heart'sWay Hospice requires and informs individuals that requests for amendment of their health information must be made in writing and that their request must include a reason supporting why the amendment should be accepted.
2. Requests will be forwarded to the Privacy Officer for review and further action.
3. If the request for amendment is not received in writing, and if the written request does not include a reason supporting the request, the Agency is not required to act upon it.
4. When a request for amendment of health information is received, it will be acted upon within 60 days. A one-time extension of 30 days is allowed if necessary and provided that the individual requesting the amendment is informed of the reason(s) for the delay and the date by which they can expect action to be taken upon their request.
5. The Agency documents the titles of the person/offices responsible for receiving and processing requests for amendment for a period of six years

When a request for amendment is denied

1. The individual is given a statement written in plain language that explains the reasons for denial and the individual's right regarding the denial decision.
2. If the individual chooses to write a statement of disagreement with the denial decision, Heart'sWay Hospice may write a rebuttal statement and will provide a copy to the individual.
3. The Agency will include the request for amendment, denial letter, statement of disagreement, and rebuttal (if any), with any future disclosures of the disputed health information.
4. If the individual does not choose to write a statement of disagreement with the denial decision, the Agency is not required to include the request for amendment and denial decision letter with future disclosures of the disputed health information unless requested by the individual.

When a request for amendment is accepted (in whole or in part)

1. Heart'sWay Hospice will identify the records that are the subject of the amendment request and will append the amendment to the record.
2. The Agency will inform the individual that their request for amendment has been accepted and request the identification of and permission to contact other individuals or health care entities that need to be informed of the amendment(s).

3. The Agency will inform the person/entities identified by the individual as well as its business associates who may require the amendment.

12.4.7.6 Right to an Accounting of Disclosures

Individuals have the right to request an accounting of the disclosures of their health information. Disclosures of PHI for treatment, payment and operations or disclosures made pursuant to a valid consent or authorization are excluded from this requirement.

Procedure:

Heart'sWay Hospice will provide an accounting of disclosures of an individual's health information for up to six years prior to the date of the individual's request. The Privacy Officer or designee is responsible for ensuring that disclosures are logged in the clinical record and providing accounting as necessary pursuant to a valid request.

When a request for an accounting of disclosures of health information is received, it will be acted upon within 60 days. A one-time extension of 30 days is allowed if necessary and provided that the individual requesting the amendment is informed of the reason(s) for the delay and the date by which they can expect action to be taken upon their request.

An individual may receive an accounting of disclosures once during any 12-month period for no charge. If an individual requests more than one accounting within the same 12-month period, a reasonable, cost-based fee of $10.00 may be charged by the Agency. The individual will be provided with the opportunity to modify or withdraw his or her request.

The accounting for each disclosure includes:

1. The date of the disclosure
2. The name of the entity or person to whom the disclosure was made and their address (if known)
3. A brief statement of the purpose of the disclosure or a copy of the individual's written authorization or a copy of the written request for the disclosure

12.4.9 Deceased Patients

Heart'sWay Hospice protects the health information of deceased hospice patients in the same manner and to the same extent as it did prior to the patient's death.

Procedure:

1. Protection of the privacy of a deceased patient's health information is provided for 50 years after the patient's death.
2. The Agency may use or disclose the PHI about individuals who have been deceased for more than 50 years for any purpose.
3. A personal representative of the deceased person (someone with legal authority to act on behalf of the deceased person or his or her estate) may exercise the deceased person's rights with respect to protected health information.
4. The identity of the personal representative and his/her authority to act on behalf of the deceased individual is verified according to standard hospice procedures.

5. Hospice may disclose information about a decedent to family members or others involved in the patient's care unless such disclosures would be inconsistent with the prior expressed preferences of the patient.

12.4.12 State Requirements

The state of Texas passed HB300 in 2011 to update chapter 181 of the Health and Safety Code. Texas felt that incentivizing the Electronic Medical Record would increase electronic exchanges and that an increase in privacy and security protection for PHI was needed. The Texas Medical Safety Act covers all entities that assemble, collect, analyze, use, evaluate, store, or transmit protected Health Information. If a healthcare provider qualifies as a HIPAA Covered Entity, they are required to comply with the HIPAA Administrative Simplification Provision unless preempted by a provision of the Texas Medical Privacy Act.

HB 300 requires establishing and maintaining a consumer information website as stipulated in Section 181.103 by the attorney general's office (Case Text, 2023b).

The website must provide certain information, including:

- Information regarding consumer privacy rights as it relates to PHI under state and federal law
- The state agencies that regulate covered entities in the state
- Detailed information regarding each agency's complaint process
- Contact information for each agency and how to report a violation

www.texasattorneygeneral.gov/consumer-protection

Texas Medical Practice Act is more stringent with higher penalties for HIPAA violations and failure to notify affected individuals of security breaches.

It is the policy of Heart'sWay Hospice Inc. to comply with state statutes and regulations that may impact on our Agency. Please consult with the Privacy Officer if you have any questions about the applicability of state requirements for our operations.

12.4.13 Sanctions

Heart'sWay Hospice applies appropriate sanctions against any staff member who violates the organization's privacy practices. Incidental disclosures that cannot be reasonably prevented, which are limited in nature, and which occur as by-product of an otherwise permissible use are not considered violations of the Agency's policies or of the HIPAA Privacy Rule.

Procedure:

1. The Agency's staff are provided with training and retraining as necessary to ensure they understand the organization's privacy practices and its expectations that staff and volunteers will adhere to them.
2. Sanctions are applied against any staff member or volunteer who violates the Agency's privacy practices.

3. Sanctions are applied in accordance with the Agency's established disciplinary procedure.
4. Any sanctions applied are documented and retained for a period of six years.
5. Sanctions are not applied against any member of Heart'sWay Hospice's workforce who engages in whistleblower activities including lodging complaints with any entity regarding violations of the Agency's privacy practices.

12.4.14 Effective Date and Transition Rules

Heart'sWay Hospice's privacy policies are effective April 14, 2003.

Transitioning for including the required privacy provisions in business associate contracts is:

- All new contracts with business associates negotiated after October 12, 2002, must include the privacy provisions
- Any contract renewals or revisions after April 14, 2003, must include the privacy provisions
- Otherwise, the Agency may operate under the terms of existing contracts up to April 14, 2004. All Agency contracts must include the privacy provisions after that date

12.5 Security of Health Information

It is the policy of Heart'sWay Hospice to preserve and protect the security and integrity of electronic health information in accordance with state law and federal regulations and sound clinical and business practices. Agency's systems and policies are to be compliant, manageable, practical and cost-effective, but not necessarily state-of-the-art.

12.5.1 IT Director

The Executive Director will appoint an IT Director who is responsible for overseeing the security and integrity of health information kept in electronic form.

The designated staff will:

1. Design, implement, monitor and update policies, systems and processes to ensure the safety and integrity of the Agency's electronic data and information systems
2. Assign unique user ID's and passwords to Agency employees and delete or inactivate access to the computer system by terminated employees
3. Provide and limit software access to protected health information on a minimum necessary basis.
4. Provide training in Agency security and acceptable use policies to new employees who will have access to the Agency's computer system and retrain as necessary and appropriate. Each employee with computer access will sign an acknowledgement that they have received and will comply with the Agency's acceptable use policies. These acknowledgements will be kept in the employee's personnel record
5. Monitor system events on a routine basis to audit potential security breaches and system malfunctions
6. Investigate suspected or confirmed security breaches and report to the Executive Director. Design and implement remedial measures as necessary and appropriate to prevent reoccurrence

7. Perform routine backups of vital Agency data. Monitor success of routine backups and keep backup media safe and secure
8. Serve as internal and external liaison and resource between the Agency, its employees and outside entities including vendors, insurance carriers and their fiscal intermediaries, oversight agencies and accrediting bodies on computer security issues
9. Design and execute disaster recovery plans to ensure prompt restoration of computer data and system availability
10. The IT Director may designate an alternate to perform important daily functions in his/her absence

12.5.2 Agency Software Systems

The mission critical software systems currently used by the Agency are:

Microsoft Windows 2019 or 2021 Server	File server operating system
Microsoft Windows 10 or 11	Workstation and laptop operating systems
WellSky Hospice	Electronic Medical Record (EMR)
CYMA Not for Profit Edition	Accounting system

Other software packages are used for non-mission critical functions.

12.5.3 System Upgrades and Policy Revisions

Approval by the Board of Directors is required for major changes in clinical information systems or accounting software. Approval by the Executive Director or designee is required for changes in other mission critical software.

Upgrades and enhancements to current software packages may be made at the discretion of the IT Director with appropriate research and testing. The security functionality of any such upgrades and enhancements shall meet or exceed the policies and practices listed herein. Likewise, the It Director may make improvements in the administration of the security provisions of existing software or install new or revised non-mission critical software at his/her discretion so long as the improvements meet or exceed the Agency security provisions.

Computer software and security practices change rapidly. The IT Director is responsible for monitoring and tracking industry trends and risks and making appropriate recommendations to the Executive Director for changes to Agency hardware/software/computer administration practices. Significant changes may require updating the Agency's security policy and retraining staff as necessary and appropriately. The IT Director will review Agency security practices and risks at least annually and recommend practical, manageable, and cost-effective improvements as appropriate.

12.5.4 Acceptable Use Policy – Workstation/Laptop Users

1. The responsible employee who is assigned to a workstation or laptop will report any loss, theft or damage to the IT Director as soon as possible.
2. Workstations are to be used for authorized Agency business only. Personal use of an unbusinesslike nature or allowing these devices to be used by anyone but an authorized Heart'sWay Hospice employee is prohibited.
3. The user agrees not to deactivate any security or maintenance functions, such as virus protection or hard disk maintenance utilities which have been installed. The user agrees to perform any such additional security or maintenance functions as instructed. The user will report any known software or hardware malfunctions to the IT Department as soon as possible.
4. Screen settings must be set so that the computer screen(s) will go blank at a minimum of 30 minutes and a password will be required to reactivate the screen(s). As an alternative the user can lock the screen manually (CTRL, Lock). A password will also be required to unlock the screen.
5. Unauthorized disclosure or use of Agency passwords or security codes will not be permitted. Employees violating this policy will be subject to disciplinary action.
6. The user agrees that any information which they enter in the computer system or which they modify will be true and correct in accordance with the professional standards for their job function and/or professional discipline.
7. The user agrees to maintain the security and confidentiality of clinical information stored on the field device in accordance with Agency policy and accepted professional standards.

12.5.5 Acceptable Use Policy – Smart Phone/Tablet

Smart phones and tablets are used extensively for agency business including entering, transmitting, or reviewing Protected Health Information. New employees have the option of using a Agency phone or using a personal phone and being reimbursed for use of the phone on agency business. Users of Agency phones are permitted to use them for limited personal use, such as personal phone calls, texts, etc., but are to refrain from high volume transmissions such as watching streaming media, games, etc. User owned phones are not limited to these restrictions, but access to PHI must be limited by the authentication process.

1. Each employee who is issued an Agency owned smart phone or tablet will exercise reasonable care to prevent the device being lost, stolen or damaged. Field devices will not be left unattended outside the office or the employee's home. Field devices will not be left in unlocked vehicles.
2. The employee who is issued a field device will report any loss, theft or damage to the IT Director as soon as possible.
3. Unauthorized disclosure or use of Agency passwords or security codes will not be permitted. Employees violating this policy will be subject to disciplinary action.
4. The user agrees that any clinical information entered into the computer system or which they modify will be true and correct in accordance with the professional standards for their job function and/or professional discipline.

5. The user agrees to maintain the security and confidentiality of clinical information stored on the field device in accordance with Agency policy and accepted professional standards.
6. Employees who resign or are terminated will return any agency owned field device and related equipment they have been issued in good working conditions. The return of this Agency property will be a condition for receiving a final paycheck and any accumulated paid time off.
7. Agency owned field devices are to be used for authorized Agency business only. Personal use of an unbusinesslike nature or allowing these devices to be used by anyone but an authorized Heart'sWay Hospice employee is prohibited.
8. Unauthorized disclosure or use of Agency passwords or security codes will not be permitted. Employees violating this policy will be subject to disciplinary action.
9. The user agrees to maintain the security and confidentiality of clinical information stored on the field device in accordance with Agency policy and accepted professional standards.

12.5.6 Additional Security

Our WellSky EMR, Microsoft Office 365 which includes secure Outlook email, Teams secure messaging and secure virtual meetings, are accessed via their cloud systems. Availability and security of essential information including PHI are protected by systems that meet or exceed established data center standards. Communications to and from the network cloud system in in place are highly encrypted

1. Each user will be issued a unique user identification and password to access the Agency's network.
2. Users requiring access to the Agency's clinical information system will be issued with separate ID and password.
3. Smart phones must be screen lock protected using a 4-digit PIN number, password or biometrics. The screen lock will go into effect a maximum of 10 minutes of the phone is being inactive.
4. Users requiring access to the Agency's accounting system will be issued with a separate ID and password.
5. The WellSky Hospice EMR system utilizes electronic signatures. A separate password is required to electronically sign a document.
6. For cloud-based applications, physical security, backups, access security, encryption, multi-site availability, software updates, backup internet access, electrical power and cooling systems, (etc.) are the responsibility of the software vendor and will comply with accepted standards.
7. The clinical system will log off users who have not been active for 20 minutes (or other time period as designated by the IT Director).

12.5.7 Transmitting Billing Information

1. Transmitting billing information to and from our Medicare fiscal intermediary will be by EDI using the intermediaries privately contracted secure internet connection.

2. Transmitting billing information to and from our Medicaid fiscal intermediary will be over the internet using their specialized secure software and EDI system.
3. Private insurance is billed electronically.
4. The CFO and staff assigned to billing and accounting will be the only personnel permitted to send and receive billing information. This is controlled by ID and password.

12.5.8 File Server and Internal Network Security

1. Only the IT Director or designee will be permitted to perform remote administration of the file server.
2. Only the IT Director will have access to the administrative password for the system.
3. A unique administrator ID and password will be required to access the system.
4. The network protocol will be TCP/IP only.

12.5.9 Physical Security

1. Workstations will generally not be used in public areas of the office except for those being used by a receptionist.
2. The outside doors to the office will be kept locked when the office is not occupied.
3. Field devices are not to be kept in unlocked vehicles.
4. File servers are kept in the server room.

12.5.10 Computer System Backups

The IT Director will make complete backups of the file server data files after the office closes each day. All medical records, billing, and accounting records will be stored on the file server and included in the daily backups. A duplicate backup will be made daily to an offsite location. Data from individual workstations will only be backed up by special need or special request. Each user will be encouraged to store sensitive or mission-critical information on the file server, where it will also be backed up.

The IT Director is responsible for monitoring the system and software log(s) on a routine basis and investigating and resolving any indicated problems as necessary and appropriate.

12.5.11 Electronic Signatures and Electronic Clinical Records

The Agency uses electronic (not digital) signatures for assessments, physician's telephone orders, Face to Face visit and CTI documentation and on the initial and updated plans of care. The Agency utilizes electronic clinical records extensively. The WellSky Hospice clinical computer system as implemented, as well as the previously listed Agency security policies, ensure consistent and ongoing protection and verification of data.

A separate user ID and password are required to access the WellSky Hospice database. Both user-based access (for the individual) and role-based access (for the user's job function) security are implemented. Users are permitted to add, modify or view specific data based on a security profile to limit access to the minimum necessary required to perform the employee's designated job function. The system administrator is the IT Director for the Agency.

12.5.12 Disaster Recovery

System backups will be made, verified and stored as specified elsewhere in this policy.

- The file servers, routers and switches are to be protected by an uninterruptible power supply (UPS). The UPS will be regularly tested.
- Workstations, peripheral devices and any other devices connected to the network cabling will be protected by high quality surge protectors.
- The It Director should utilize standard “off the shelf” components that can be repaired or replaced by any of several local vendors or mail order businesses on a priority basis.

The Security Officer is responsible for disaster recovery and emergency access to computer functions. The above policies will permit the IT Director to recover from a disaster on a timely basis and protect against loss of mission critical data.

12.5.13 WellSky Security Practices

Our EMR was changed to WellSky Hospice on February 1, 2019. This is a cloud-based system accessible over the internet. WellSky file servers are in a dedicated secure rack, which is only accessible to WellSky employees. The datacenter building has guaranteed HVAC, power and network connectivity, even in the event of an extended power outage. Biometric credentials are required for building access.

WellSky runs incremental backups on the production database every four hours each day, as well as a full backup of the database nightly. Backups are restored on a separate database server to ensure the data integrity of the database backups. WellSky transfers a full backup of the application data to a secure, off-site backup location each week. In addition, a full backup will be transferred to the off-site location at any time the datacenter might be vulnerable to a natural disaster. A full backup was transferred off-site, for example, when Hurricane Ike was a potential threat to Houston.

For active clients, WellSky maintains and archives all electronic data. This data is secured using forward-encrypted user passwords and housed in a secure production infrastructure. All data uses 256-bit encryption while in electronic transit. Archived and back-up media is stored in a secure, and geographically separate, location from their production environment. The backup media is secured with an encryption algorithm certified by the National Institute of Standards and Technology (AES 256-bit key encryption). Should the Agency decide to change to another EMR computer system, WellSky has agreed to maintain our data and access to such data for up to six years.

WellSky is fully responsible for software updates, server hardware and software maintenance and upgrades, virus protection and internal security.

12.5.14 Heart’sWay Security Policy Utilizing WellSky Hospice

Policy: Heart’sWay Hospice staff may use electronic signatures on all computer-generated documentation. An electronic signature will serve as authentication on patient record documents generated via the organization's WellSky application. It is the policy of HeartsWay Hospice to ensure that protected health information is private, secure, and available in accordance with all HIPAA/Hi-Tech standards.

Procedure:

1. Heart'sWay Hospice staff may create patient documentation via computer system.
2. For the purpose of the electronic medical record, and documents printed from the electronic medical record, the employee's use of a separate Electronic Signature Passcode after authenticating with her/his system this electronic signature serves as her/his legal signature.
3. The organization-based application administrator will issue each employee a system Username and a temporary password. The user will create a new password upon initial log in to the organization's WellSky application.
4. The employee will generate an Electronic Signature Passcode that will only be accessible to her/him.
5. Each user will be required to change her/his Log in Authentication Password every 60 days.

12.5.15 Sanctions

Heart'sWay Hospice applies appropriate sanctions against any staff member who violates the organization's security practices. Incidental or one-time breaches that cannot be reasonably prevented, which are limited in nature, and which occur as a by-product of an otherwise permissible activity, are not considered violations of the Agency's policies.

Procedure:

1. The Agency's staff are provided with training and retraining as necessary to ensure they understand the organization's security practices and their expectations that staff will adhere to them.
2. Sanctions are applied against any staff member or volunteer who violates the Agency's security practices.
3. Sanctions are applied in accordance with the Agency's established disciplinary procedure.
4. Sanctions are not applied against any member of Heart'sWay Hospice's workforce who engages in whistleblower activities including lodging complaints with any entity regarding violations of the Agency's security practices.

12.5.16 Breach notification Requirements

Definitions:

Breach – means the acquisition, access, use or disclosure of protected health information in a manner not permitted in the Privacy Rule which compromises the security or privacy of the protected health information.

Unsecured protected health information – protected health information that is not rendered unusable, unreadable or indecipherable by encryption or destruction.

Affected individual – the person whose PHI was breached.

Procedure:

1. All incidents related to a suspected or actual breach of unsecured protected health information are reported to the IT Director as soon as discovered.
2. An immediate investigation is conducted, and the Breach Risk Assessment is completed and its findings documented in the Breach Risk Assessment Summary
3. Based on the findings of the investigation and the Brach Risk Assessment, a determination is made regarding whether there is a probability that the protected health information has been compromised and therefore constitutes a reportable breach.
4. If the incident does not constitute a reportable breach, the IT Director will retain the documented findings for six years from the date the incident occurred.
5. If a reportable breach has occurred, relevant information is gathered for the breach notification letter to be sent to affected individuals as soon as possible but no later than 60 calendar days from the date of the discovery of the breach. HB 300 amended the relevant section of the Business and Commerce Code to require entities covered by the Medical Privacy Act to notify residents even if the agency outside of Texas. Covered entities are also required to notify the Texas Attorney General of all data breaches affecting 250 or more Texas residents.
6. The written breach notification letter is sent by first class mail to the last known address of the affected individuals(s).
7. If the affected individual is deceased, the written notification letter may be sent to the individual's next of kin or personal representative if their contact information is available.
8. If the affected individual is deceased and contact information for next of kin or the personal representative is inaccurate or unavailable, no further notification is required although the breach will be included in the Agency's accounting of reportable breaches to the government.
9. If the Agency is unable to reach more than 10 of the affected individuals, the Agency will post a conspicuous notification on its web site for 90 days and/or notify media in the locations(s) where the affected individuals are believed to reside.
10. If a breach affects more than 250 individuals in a specific state or jurisdiction, prominent media outlets will be contacted no later than 60 calendar days of the discovery of the breach, and a prominent notice will be placed on the Agency's web site in addition to the individual notification of affected individuals.
11. If more than 250 individuals are affected by a breach, the Agency will notify Texas Attorney General within 60 calendar days of discovery of the breach following the instructions posted on its web site.
12. For each breach that is discovered within a calendar year that affects less than 250 individuals, the Agency will maintain documentation of all information related to the breach and its investigation and provide an accounting of all such breaches to Texas Attorney General within 60 days following the end of the calendar year. This accounting is provided in accordance with instructions posted on The Texas Attorney General's website.
13. All documentation related to all breaches discovered by the Agency or any of its business associates is maintained for six years from the date of discovery of the breach.