Policy Number: PP 2.0

Policy Title: Privacy Policy and Procedures

Policy Statement/Purpose: The Company written policies and procedures that describe relevant regulations and how they should be implemented. This policy is subject to the requirements, prohibitions, and safe harbors of Company's No Information Blocking policy. (See Policy 1.0.0)

Policy Interpretation and Implementation: The Privacy Officer is responsible for developing and maintaining all privacy-related policies and procedures. Written policies and procedures are reviewed and revised periodically to reflect changes to Company business practices as well as changes to applicable laws, rules, and regulations. Revised policies and procedures shall become effective upon approval by the Privacy Officer and Privacy Committee. This policy is subject to the requirements, prohibitions, and safe harbors of Company's No Information Blocking policy. (See Policy 1.0.0)

A. CONFIDENTIALITY OF PERSONAL HEALTH INFORMATION

1). Overview: The Company protects personal health information to ensure that residents are not afraid to seek healthcare or to disclose sensitive information to The Company. Personal health information is protected during its collection, use, disclosure, storage, and destruction within The Company in accordance with the provisions of state and federal regulations.

2). Definitions:

a. **Personal Health Information (PHI)** – All information, recorded or exchanged verbally about an identifiable patient:
   1. That can identify an individual including, but not limited to, name, birthdate, social security number, diagnosis, or medical record number. The patient's health and healthcare history, including genetic information about the patient or the patient's family.
   2. What The Company has learned or observed, including conduct or behavior that may be a result of illness or the effect of treatment.
   3. The provision of healthcare to the patient.
   4. Payment for healthcare provided to the patient, and includes:
      - The Personal Health Identification Number and any other number, symbol, or identifier assigned to a patient
      - Any identifying information about the patient that is collected during, and is incidental to, the provision of healthcare or payment for healthcare
   5. The patient's personal information, including financial position, home conditions, domestic difficulties, or any other private matters relating to the patient which have been disclosed to staff or persons associated with The Company.

b. **Electronic Access -** means an internet-based method that makes EHI available at the time the EHI is requested and where no manual effort is required to fulfill the request.

c. **Electronic Health Information (EHI) -** means Electronic Protected Health Information contained in a Designated Record Set. It does not include Psychotherapy Notes or information compiled in anticipation of or for use in a civil, criminal, or administrative

action or proceeding. EHI also excludes any information that has been de-identified in accordance with HIPAA's de-identification standards. And until May 2, 2022, the definition of EHI may be further limited to those data elements represented in the USCDI (version 1).

d. **Privacy Officer** – The employee, designated by The Company, whose responsibilities include dealing with requests from residents who wish to examine and copy, or to collect, personal health information collected and maintained by The Company.
e. **Persons Associated with The Company** – Includes all contracted individuals, volunteers, students, researchers, Company Medical Staff, members of the Governing Body of The Company, information managers, employees of The Company, Business Associates, or agents of any of the above.
f. **Information Manager** – The individual, corporate organization, business, or association who processes, stores, or destroys personal health information for The Company, or provides information management or information technology for The Company.

3). Confidentiality of Personal Health Information:

a. All Company employees and Persons Associated with The Company are responsible for protecting the security of all personal health information (oral or recorded in any form) that is obtained, handled, learned, heard, or viewed during his or her work or association with The Company.
b. Personal health information shall be protected during its collection, use, storage, and destruction within The Company.
c. Use or disclosure of personal health information is acceptable only in the discharge of one's responsibilities and duties (including reporting duties imposed by legislation) and based on the need to know except where otherwise prescribed by the Company's No Information Blocking Policy. Discussion regarding personal health information shall not take place in the presence of persons not entitled to such information or in public places (elevators, lobbies, cafeterias, off premises, etc.) or on social media sites.
d. The execution of a Personal Health Information Privacy Plan Acknowledgment (PP Appendix 2.0.1 C *Acknowledgement of The Company Privacy Plan*) is required as a condition of employment with The Company and signed:
    1. At the commencement of their relationship with The Company
    2. Each time there is a substantial change in an individual's position, as determined by the department, program, or division responsible for the individual
    3. For reasons, and at intervals as deemed appropriate by the department, program, or division
e. Unauthorized use or disclosure of confidential information, except where otherwise prescribed by the Company's No Information Blocking Policy, shall result in a *disciplinary response* up to and including termination of employment. A person convicted of an offense under the Health Insurance Portability and Accountability Act may be required to pay a fine. A confirmed breach of confidentiality may be reported to the individual's professional regulatory body.
f. All individuals who become aware of a possible breach of the security or confidentiality of personal health information shall follow the procedures outlined in the "Procedure if a Breach is Alleged" section below.

4). Privacy Plan Acknowledgement Procedure:

a. All Company employees, as a condition of employment, shall sign a *Privacy Plan Acknowledgment*. Administration of this pledge is handled by the employee's department, program, or division and the original forwarded to the employee's Human Resources file. The Privacy Officer shall retain a copy.
b. All contractors engaged in providing a service for The Company, where the service provided would expose them to confidential information shall sign a *Privacy Plan Acknowledgment*. The administration of this pledge is handled by the individual in charge of contracts and the original retained by that individual. The Privacy Officer shall retain a copy.
c. All Company Governing Body members shall sign a *Privacy Plan Acknowledgment*. The administration of this pledge is handled by the Corporate Secretary who shall retain the original. The Privacy Officer shall retain a copy.
d. All Company agents who are regularly associated with The Company shall sign a *Privacy Plan Acknowledgment*. The administration of this pledge is handled by Human Resources and the original retained by Human Resources. The Privacy Officer shall retain a copy.
e. All employees of other agencies (such as nurses from temporary agencies, or employees in physicians' billing offices) who regularly associate with The Company shall sign a *Privacy Plan Acknowledgment*. The administration of this pledge is handled by the Department with which the agency has an association and the original retained in that Department. The Privacy Officer shall retain a copy.

B. Safeguarding Protected Health Information

1). *Overview:* The Company is committed to compliance with privacy laws, rules, and regulations. As such, The Company provides guidelines for safeguarding Protected Health Information (PHI) and to limit unauthorized disclosures of PHI except where required by the Company's No Information Blocking Policy. The Company shall have in place appropriate administrative, physical, and technical safeguards to protect the privacy of PHI as required by HIPAA and/or state privacy laws in accordance with the Company's No Information Blocking Policy.

The Company shall ensure, to the extent possible, that PHI is not intentionally or unintentionally used or disclosed in a manner that would violate the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or any other federal or state regulation governing confidentiality, privacy, and disclosure of health information.

2). *Procedure:*

a. The Company shall implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements, considering:
    1. The size, complexity, and capabilities of The Company
    2. The Company's technical infrastructure, hardware, and software security capabilities
    3. The costs of security measures
    4. The probability and criticality of potential risks to Electronic Protected Health Information (ePHI)

b. The Company may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with applicable laws, rules, and regulations.
c. The Company shall maintain the policies and procedures in written (which may be electronic) form and, if an action, activity, or assessment is required to be documented, it shall be maintained in written (which may be electronic) form.
d. The Company shall retain all documentation for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. This includes policies and procedures as well as records relating to implementation, such as log-in audit information, logs of security incidents, and documentation of training.
e. The Company shall make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
f. The Company shall review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the e-PHI.
g. Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information it holds.
h. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
i. Identify an employee as a Privacy Officer/Security Manager who is responsible for the development and implementation of these policies and procedures.
j. Apply appropriate sanctions against workforce members who fail to comply with The Company's security policies and procedures.
k. Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

3). *Oral Disclosures:* Reasonable measures shall be taken to assure that unauthorized persons do not overhear conversations involving PHI.

4). *Written Disclosures:* All documents containing PHI shall be stored appropriately to reduce the potential for incidental use or disclosure. Documents shall not be easily accessible to any unauthorized staff or visitors.

5). *Computer Access:*
a. Only staff members who need to use computers to accomplish work-related tasks shall have access to computer workstations or terminals.
b. All users of computer equipment must have unique login and passwords.
c. It is recommended that passwords be changed every ninety (90) days.
d. Posting, sharing, and any other disclosure of passwords and/or access codes is **strongly discouraged.**
e. Access to computer-based PHI shall be limited to staff members who need the information for treatment, payment, or healthcare operations.
f. Staff members shall log off their workstation when leaving the work area.
g. Computer monitors shall be positioned so that unauthorized persons cannot easily view information on the screen.

h. Employee access privileges will be removed promptly following their departure from employment.
i. Employees will immediately report any violations of this Policy to their supervisor or Privacy Officer/Security Manager.

6). *Printers, Copiers, and Fax Machines*:

a. Printers and fax machines will be in areas not easily accessible to unauthorized persons.
b. If equipment cannot be relocated to a secure location, a sign will be posted near the equipment indicating that unauthorized persons are prohibited from viewing documents from the equipment. Sample language: "Only authorized staff may view documents generated by this (indicate printer, copier, fax, etc.). Access to such documents by unauthorized persons is prohibited by federal law."
c. Documents containing PHI will be promptly removed from the printer, copier, or fax machine and placed in an appropriate and secure location.
d. Documents containing PHI that must be disposed of due to error in printing will be destroyed by shredding or by placing the document in a secure recycling or shredding bin until destroyed.

7). *Destruction:*

Written: Documentation shall be destroyed promptly when it is no longer needed by shredding or placing the information in a secure recycling or shredding bin until the time that it is destroyed.

Electronic: Prior to the disposal of any computer equipment, including donation, sale, or destruction, The Company must determine if PHI has been stored in this equipment and will delete all PHI prior to the disposal of the equipment.

8). *Monitoring Compliance:* Compliance with The Company's privacy policies and procedures shall be monitored on an ongoing basis to ensure compliance. In the event The Company identifies noncompliance through report or audit, the Privacy Officer shall immediately investigate and correct the noncompliance as well as put into place necessary corrective action, such as review and modification of policies and procedures as well as training for appropriate individuals.

C. MINIMUM NECESSARY

1). *Overview:* The HIPAA Privacy Rule requires The Company to make reasonable efforts not to use or disclose more than the minimum amount of Protected Health Information (PHI) necessary to accomplish the intended purpose of the use, disclosure, or request, taking into consideration practical and technological limitations. When using or disclosing PHI, or when requesting PHI from another covered entity or business associate, The Company must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request in accordance with the HIPAA Privacy Rule and the Company's No Information Blocking Policy.

The Company has processes in place to implement policies and procedures that comply with the Minimum Necessary provision of the Health Insurance Portability and Accountability Act

of 1996 (HIPAA). Minimum necessary provisions do not apply to treatment. Healthcare cannot stop while decisions are being made. Healthcare often requires easy access to information, especially in urgent or emergent situations. The HIPAA Privacy Rule minimum necessary standard also does not apply to the following:

a. Disclosures to or requests by a health care provider for treatment purposes.
b. Disclosures to the individual who is the subject of the information.
c. Uses or disclosures made pursuant to an individual's authorization.
d. Uses or disclosures required for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Rules.
e. Disclosures to the Department of Health and Human Services (HHS) when disclosure of in-formation is required under the Privacy Rule for enforcement purposes.
f. Uses or disclosures that are required by other law.

2). *Procedure:* All new workflow and information systems are designed/acquired to meet the minimum necessary provisions of HIPAA. The Company removes identifiers and removes data fields that are not necessary to fit the purpose of the use or disclosure.

a. Diagnoses do not generally have to be exposed to administrators dealing with billing amounts.
b. The De-Identification and Establishing Access Control policies and procedures are the principal policies and procedures through which the minimum necessary provisions are implemented.
c. The Privacy Officer will review the compliance with the Minimum Necessary provisions annually and recommend actions to senior management.
d. When using or disclosing PHI subject to the HIPAA Privacy Rule minimum necessary standard, The Company must identify those persons or classes of persons, as appropriate, in its workforce who need access to PHI to carry out their duties and, for each such person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access.
    1. The Company shall limit access to PHI to that which is appropriate for the person or class of persons to carry out their duties.
    2. The Company shall review requests for disclosure on an individual basis to ensure that the PHI disclosed is limited to the amount reasonably necessary to achieve the purpose of the disclosure.
    3. The Company shall limit any request for protected health information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities.
        - The Company shall not use, disclose, or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request and in accordance with the Company's No Information Blocking Policy.
e. The Company may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:
    1. Making disclosures to public officials, so long as (1) the disclosure is otherwise permitted under The Company policies and procedures as well as applicable laws, rules, and regulations, and (2) the public official represents to The Company in writing that the information requested is the minimum necessary for the stated purpose

2. The information is requested by another covered entity
3. The information is requested by a professional who is a member of The Company's workforce or is a business associate of The Company for the purpose of providing professional services to The Company, so long as the professional represents that the information requested is the minimum necessary for the stated purpose
4. The requested EHI is required to be released pursuant to the Company's No Information Blocking Policy and is not protected under the policy's safe harbors.

f. Exceptions to the Minimum Necessary Requirement:
1. Disclosures to, or requests by, a healthcare provider for treatment
2. Uses or disclosures made to the individual
3. Uses or disclosures made pursuant to a valid authorization
4. Disclosures made to the Secretary HHS
5. Uses or disclosures that are required by law including, but not limited to, the 21st Century Cures Act and its Information Blocking Rule
6. Other uses and disclosures that are required for compliance with HIPAA requirements

Employees who use or access PHI for reasons not related to their job duties, or who disclose PHI to any party for any reason not related to their job duties and in violation of state and federal law shall be subject to discipline, up to and including termination.

D. USES AND DISCLOSURES TO CARRY OUT TREATMENT, PAYMENT, OR HEALTHCARE OPERATIONS

1). *Overview:* The Company may use or disclose PHI for treatment, payment, or healthcare operations, unless the use/disclosure requires authorization or is prohibited by law, rule, or regulation. The Company provides guidance for uses and disclosures of Protected Health Information (PHI) that do not request consent.

Designated types of medical records are considered more sensitive and, therefore, are not governed by this policy: communicable disease information (including HIV/AIDS information), mental health records, genetic testing information, and drug and alcohol abuse records.

2). *Procedure:*
a. Before disclosing PHI for treatment, payment, or healthcare operations, The Company must verify the identity and authority of the recipient, in accordance with The Company's policy.
b. The Company shall disclose the minimum necessary amount of PHI, in accordance with The Company's policy.
c. The Company may, but need not, obtain consent of the individual to use or disclose PHI to carry out treatment, payment, or healthcare operations.
1. Consent is not effective to permit the use or disclosure where authorization is required.

3). *Definitions*:
Treatment - Provision, coordination, or management of healthcare and related services by one or more healthcare providers, including the coordination or management of healthcare by a

healthcare provider with a third party; consultation between healthcare providers relating to a patient; or the referral of a patient for healthcare from one healthcare provider to another.

Payment - Activities undertaken by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or activities by a healthcare provider or health plan to obtain or provide reimbursement for the provision of healthcare, including but not limited to determining eligibility or coverage; coordination of benefits; adjudication or subrogation of health benefit claims; risk adjusting amounts due based on enrollee health status and demographic characteristics; billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related healthcare data processing; review of healthcare services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and disclosure of certain information to consumer reporting agencies.

Healthcare Operations - Any of the following activities undertaken by The Company:

a. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, except where the primary purpose is research.
b. Reviewing the competence or qualifications of healthcare professionals; evaluating practitioner and provider performance, and health plan performance; conducting training programs in which students, trainees, or practitioners in areas of healthcare learn under supervision to practice or improve their skills as healthcare providers; training of non-healthcare professionals; and accreditation, certification, licensing, or credentialing activities.
c. Underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for healthcare (including stop-loss insurance and excess of loss insurance).
d. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs.
e. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies.
f. Business management and general administrative activities of the entity including, but not limited to:
    1. Management activities relating to implementation of, and compliance, with the requirements of this subchapter
    2. Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer
    3. Resolution of internal grievances
    4. The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that, following such activity, will become a covered entity and due diligence related to such activity

5. Creating de-identified health information or a limited data set
6. Fundraising for the benefit of The Company

E. SECURING CONSENT/RESTRICTIONS/REQUESTS

1). *Overview:* The Company may request that residents sign an acknowledgment form, explaining that The Company may use or disclose protected health information to carry out treatment, payment, or healthcare operations prior to the use or disclosure. The form shall also refer to the Notice of Privacy Practices (Refer Appendix PP 2.0.1, Section C, *Privacy Plan Acknowledgment Form*).

The Company communicates Protected Health Information (PHI) through various means to ensure confidentiality.

2). *Procedure:* The law currently does not require that The Company obtain a signed consent for treatment, payment, or healthcare operation purposes. However, obtaining the resident's signature on an acknowledgment form ensures that the resident is aware of the provider's option to use or disclose health information for treatment, payment, or healthcare operation purposes. Additionally, it informs the resident of his/her right to request that the use or disclosure of his/her health information be restricted in some way.

Residents have the right to request that The Company communicate with them about PHI by alternative means or at alternative locations, for the communications to remain confidential. The Company shall accommodate all requests.

a. The Company must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of PHI from The Company by alternative means or at alternative locations.
b. All requests for confidential communications must be in writing.
c. The Company shall not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.
d. The Company may condition the provision of a reasonable accommodation on:
    1. when appropriate information as to how payment, if any, will be handled; and
    2. whether resident has an alternative address or other acceptable method of contact.

3). *Requests for Restriction of Use and Disclosure:* Residents may ask to restrict the way in which their health information is used or disclosed. The request must be in writing and signed and dated by the same person that signed the consent unless he or she is incapacitated. The Privacy Officer, or his or her designee, must receive the written request and determine whether it will be approved. If approved, The Company must implement the restriction. Otherwise, the person asking to restrict the use of information must be sent a denial letter. If The Company does agree to a restriction that you request, such restriction will be binding.

In any case, the Privacy Officer, or his or her designee, will retain the original and a copy of the denial letter if this should be necessary.

4). *Termination of a Restriction of Use and Disclosure:* The Company may terminate its agreement to a restriction if:

a. The resident agrees to or requests the termination in writing
b. The resident orally agrees to the termination and the oral agreement is documented
c. The Company informs the resident that it is terminating its agreement to a restriction, except that such termination is only effective with respect to protected health information created or received after the resident has been so informed

If the above criteria are met, the consent will be amended to remove the restriction.

5). *Revocation of Consent:* Residents have the right to revoke a previously signed consent. The request must be in writing and signed by the same person who signed the consent unless he or she is incapacitated. The Privacy Officer, or his or her designee, must receive the written request and determine whether it is complete. If approved, the Privacy Officer, or his or her designee, will cancel the consent; otherwise, the person asking to restrict the use of information will be sent a denial letter. In any case, the Privacy Officer will retain the original and a copy of the denial letter should one be necessary.

F. USES AND DISCLOSURES REQUIRING *OPPORTUNITY TO AGREE OR OBJECT*

1). *Overview:* The Company may use or disclose Protected Health Information (PHI), provided that the individual is informed in advance of the use or disclosure and can agree, prohibit, or restrict the use or disclosure, in accordance with applicable laws, rules, and regulations.

The Company may orally inform the individual of and obtain the individual's oral agreement or objection to an otherwise permitted use or disclosure.

2). *Procedure:* To ensure the security of PHI, The Company must:
a. ensure the confidentiality, integrity, and availability of all PHI that The Company creates, receives, maintains, or transmits;
b. protect against any reasonably anticipated threats or hazards to the security of such information;
c. protect against any reasonably anticipated uses or disclosures of such information that are not permitted by or required under HIPAA; and
d. ensure compliance by its workforce.

G. USES AND DISCLOSURES FOR CARE AND NOTIFICATION PURPOSES

1). *Overview:* The Company may use or disclose Protected Health Information (PHI), provided that the individual is informed in advance of the use or disclosure and can agree, prohibit, or restrict the use or disclosure, in accordance with applicable laws, rules, and regulations.

The Company may orally inform the individual of and obtain the individual's oral agreement or objection to an otherwise permitted use or disclosure.

2). *Permitted Uses and Disclosures:*
a. The Company may disclose to a family member, other relative, close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to

such person's involvement with the individual's healthcare or payment related to the individual's healthcare.

b. The Company may use or disclose PHI to notify or assist in the notification of (including identifying or locating), a family member, personal representative of the individual, or another person responsible for the care of the individual, of the individual's location, general condition, or death, consistent with this policy.
    1. Uses and Disclosures for Disaster Relief Purposes: The Company may use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for coordinating with such entities the use of disclosure for the abovementioned purposes.
        - If the individual is present, The Company shall comply with the requirements set forth below.
        - If the individual is not present, The Company may, in the exercise of professional judgment, determine whether the disclosure is in the best interest of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's care or payment related to the individual's healthcare or needed for notification purposes.

3). *Uses and Disclosures with Individual Present:*

a. If the individual is present for, or otherwise available prior to, a use or disclosure permitted by this policy, and has the capacity to make healthcare decisions, The Company may use or disclose the PHI if it:
    1. obtains the individual's agreement;
    2. provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
    3. reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

4). *Limited Uses and Disclosures when the Individual is Not Present:* If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, The Company may, in the exercise of professional judgment, determine whether the disclosure is in the best interest of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's care or payment related to the individual's healthcare or needed for notification purposes except where otherwise prescribed by the Company's No Information Blocking Policy.

5). *Uses and Disclosures when the Individual is Deceased:* If the individual is deceased, The Company may disclose to a family member, other relative, close personal friend of the individual, or any other person identified by the individual, who was involved in the individual's care or payment for healthcare prior to the individual's death, PHI of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known by The Company.

The HIPAA Privacy Rule allows disclosure of deceased residents' PHI to healthcare providers for the purposes of treatment. If the PHI about the deceased resident is relevant to the treatment of a family member, the family member's healthcare provider may obtain that information.

PHI about a deceased resident must be protected in the same manner and to the same extent as required for the PHI of living residents.

Executors, administrators, or other persons who have authority to act on behalf of a deceased resident must be treated as a personal representative with respect to PHI. In other words, The Company must treat the personal representative of a resident as the resident.

The Company may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, x-rays, or other similar forms of PHI.

H. REQUESTS FOR AMENDMENTS

1). *Overview:* A patient has the right to have The Company amend PHI or a record about the resident in a designated record set for as long as the PHI is maintained in the designated record set. The Company will support a resident's right to request an amendment of Protected Health Information (PHI).

2). *Request for Amendments:*

a. All requests for amendment shall be in writing to the Privacy Officer.
b. The Company may require residents to provide a reason to support a requested amendment if it informs residents in advance of such a requirement.
c. Timely action by the covered entity:
    1. The Company must act on the resident's request for an amendment no later than sixty (60) days after receipt of such a request, as follows:
        - If The Company grants the requested amendment, in whole or in part, it must make the amendment and notify the resident that the amendment has been accepted
            - The Company shall obtain the resident's identification of an agreement to have the covered entity notify the relevant persons with which the amendment needs to be shared
        - If The Company denies the requested amendment, in whole or in part, it must provide the resident with a written denial, as outlined below
        - If The Company is unable to act on the amendment within thirty (30) days, The Company may extend the time for such action by no more than thirty (30) days provided that:
            - The Company provides the resident with a written statement of the reasons for the delay and the date by which The Company will complete its action on the request; and
            - The Company shall have only one such extension.

3). *Denial of Amendment:* The Company may deny a resident's request for amendment, if it determines that the PHI or record that is the subject of the request:

a. was not created by The Company, unless the resident provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
b. is not part of the designated record set;
c. would not be available for inspection (i.e., is a psychotherapy record or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding); or
d. is already accurate and complete.

If The Company denies the requested amendment, in whole or in part, The Company must provide the resident with a timely, written denial. The denial must use plain language and contain:

a. the basis for the denial;
b. information regarding the resident's right to submit a written statement disagreeing with the denial and how the resident may file such a statement;
c. a statement that, if the resident does not submit a statement of disagreement, the resident may request that The Company provide the resident's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and
d. a description of how the resident may complain to The Company or to the Secretary of HHS. The description must include the name, or title, and telephone number of the Privacy Officer.

The Company shall permit the resident to submit to the covered entity a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement.

a. The Company may reasonably limit the length of a statement of disagreement.

The Company may prepare a written rebuttal to the resident's statement of disagreement. Whenever such a rebuttal is prepared, The Company shall provide a copy to the resident who submitted the statement of disagreement.

4). *Recordkeeping:* The Company must, as appropriate, identify the record or PHI in the designated record set that is the subject of the disputed amendment and append, or otherwise link, the resident's request for an amendment, The Company's denial of the request, the resident's statement of disagreement, if any, and The Company's rebuttal, if any, to the designated record set.

5). *Future Disclosures:*

a. If a statement of disagreement has been submitted by the resident, The Company shall identify the record or PHI in the designated record set that is the subject of the disputed amendment and append, or otherwise link, the resident's request for an amendment, The Company's denial of the request, the resident's statement of disagreement, if any, and The Company's rebuttal, if any, to the designated record set.

1. Alternatively, at the election of The Company, an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates.

b. If the resident has not submitted a written statement of disagreement, The Company shall include the resident's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the PHI only if the resident has requested such action.

6). *Actions on Notices of Amendment from Other Covered Entities:* Where The Company is informed by another covered entity of an amendment to a resident's PHI, The Company must amend the PHI in designated record sets in accordance with the amendment.

The Company shall document the titles of the persons or offices responsible for receiving and processing requests for amendments by residents and retain the documentation.

I. *REPORTING* PRIVACY CONCERNS

1.) *Overview:* The Company Privacy Program rests on the ability of staff to openly and freely communicate issues of concern to their supervisors, the Privacy Officer, and the Privacy Committee. The Company is committed to developing and supporting all lines of communication to support our efforts to detect, address, and prevent privacy breaches, including a method of anonymous reporting.

2). *Implementation:* The Company has established reporting procedures, readily accessible to all employees, vendors, executives, governing body members, and residents. Reports of privacy concerns and breaches are taken seriously and investigated accordingly. This policy includes reporting intimidation or retaliation to the Privacy Officer.

The Company's Privacy Officer is contacted with questions about applicable laws, rules, or regulations, or to report potential breaches or any concerns regarding privacy. To the extent possible, all communications to the Privacy Officer will remain confidential.

Should any individual feel uncomfortable making a report to the Privacy Officer, he/she has the option of making a report to The Company Compliance Hotline (800-557-1066), which allows for anonymous reporting of issues without fear of retribution. Signs with information for contacting the Hotline are visible throughout The Company.

All reports must be made in good faith. There will be no adverse action or retaliation against any staff member who makes a good faith report of a privacy concern. (Reference CP 2.0, *Section B, Compliance Reporting System).*

J. *RESPONDING* TO PRIVACY CONCERNS

1). *Overview:* The Company takes reasonable steps to respond appropriately to a privacy offense and prevent future similar offenses. The Company has established a system for responding to privacy issues as they arise, including investigating, retaining legal consultation, updating

policies and procedures, implementing corrective action plans, notifying affected individuals, and, when appropriate, reporting misconduct to local media as well as appropriate authorities. It is the responsibility of all associated with The Company to assist in resolving issues by participating in good faith in The Company's response to potential breaches, including cooperating when The Company is conducting investigations and abiding by corrective action.

2). *Responding:* Reports received through either a reporting mechanism or through some other mechanism shall be documented and assessed initially by the Privacy Officer. If the initial assessment indicates that there is a basis for believing that the conduct reported constitutes a breach, the matter shall be reported to the Privacy Committee for review.

All alleged breaches shall be evaluated carefully to determine whether the allegation appears to be well-founded. The Privacy Officer shall promptly begin an investigation in accordance with the following procedure:

a. Privacy Officer shall commence an investigation as soon as reasonably possible, but in no event more than thirty (30) days following reasonable suspicion of an alleged breach
b. The investigation shall include a risk assessment to determine whether a breach took place

Every effort to investigate an alleged breach shall be documented and kept with the original report.

If there was a breach, Privacy Officer shall determine, depending on the number of individuals affected:

a. Appropriate notification to affected individuals
b. Reporting to appropriate officials
c. Reporting to local media, if appropriate

3). *Corrective Action:* Corrective action shall be imposed to assist Company employees, vendors, or business associates to understand specific issues and reduce the likelihood of future breaches. Corrective action, however, shall be sufficient to effectively address the instance of breach, and should reflect the severity of the breach and/or the past adherence to standards.

The corrective action plan should identify the nature of the breach and immediate correction of any harm resulting from the breach, as well as the resolution of specific problems identified. The plan may include:

a. A recommendation to revise applicable policies and procedures to clarify proper protocols and/or development of new systems to safeguard against future breaches of a similar nature
b. Additional mandatory training for employees, contractors, vendors, and/or business associates
c. Focused review of records made by employees, contractors, vendors, or business associates for a defined period following discovery of breach
d. A recommendation to report to appropriate authorities
e. Enforcement of disciplinary standards
f. Other reasonable corrective measures calculated to ensure adherence to applicable federal and state laws, rules, regulations, and The Company Program

For a defined period following the implementation of a corrective action plan, the Privacy Officer shall follow up and audit the corrective action to determine whether it is being followed as well as its effectiveness in preventing the recurrence of similar breaches.

If an alleged breach is not substantiated, the Privacy Officer shall keep a clear record of the investigation's conclusion as well as what factors were considered in making that determination. (Reference CP 2.0, *Section H, Compliance Response and Prevention).*

K. Breach Discovery and Notification

1). *Overview:* The Company shall notify appropriate individuals and entities, following the discovery of a breach of unsecured Protected Health Information (PHI).

2). *Procedure:*

a. An allegation of a breach of confidentiality of Protected Health Information (PHI) may be made to any Company staff member/healthcare professional. Any individual receiving an allegation of a breach of confidentiality or having knowledge or a reasonable belief that a breach of confidentiality of PHI may have occurred, shall immediately notify his/her supervisor, or where this is not possible, shall notify The Company's Privacy Officer or designee. The person so notified shall in turn, notify the supervisor of the alleged violator of this policy and The Company's Privacy Officer or designee.
b. The supervisor and/or Human Resources, in consultation with the Privacy Officer, or designee, shall decide whether to proceed with an investigation. It may be decided that a complaint does not require investigation if, after consultation, the consultees believe:
    1. the subject matter of the complaint is trivial, or the complaint is not made in good faith or is frivolous; or
    2. the circumstances of the complaint do not require investigation.
c. If the decision is made to proceed with an investigation, it shall be the responsibility of the supervisor, in consultation with the Privacy Officer, or designee, to investigate the allegation (this process will include obtaining the alleged violator's version of events), consult with the appropriate resources, document findings, and make a determination as to whether there has been a breach of confidentiality of PHI.
d. If it is determined that a breach of confidentiality of PHI has occurred, disciplinary action, up to and including termination, shall be taken. Such action may include termination of employment/contract/association/appointment with The Company. The supervisor shall consult with the designated representative in Human Resources and the Privacy Officer or designee, to establish the appropriate level of disciplinary action to be applied.
e. The Company's Privacy Officer shall be informed in writing of all allegations that have been made and their outcome and shall maintain a database of this information. (Reference CP 2.0 Section, I. *Compliance Investigation)*

3). *Determining Discovery of a Breach*:

a. A breach is discovered as of the first day on which the breach is known to The Company, or, by exercising reasonable diligence, would have been known to The Company.
b. A breach is discovered if the breach is known, or, by exercising reasonable diligence, would have been known to any person, other than the person committing the breach, who is a workforce member or agent of The Company.

4). *Breach Notification:* For a breach of unsecured PHI involving fewer than five hundred (500) individuals in a state or jurisdiction, The Company shall:

a. Notify the affected individual(s) within sixty (60) days
b. Breach notification shall be made through written notice, in plain language, and shall include the following, to the extent possible:
    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 covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches
    5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, website, or postal address
c. Notice shall be sent by first-class mail to the individual's last known address, or if the individual agrees to electronic notice (and such agreement has not been withdrawn), by electronic mail
d. Insufficient or Out-of-Date Contact Information: If insufficient or out-of-date information precludes written notification, substitute notification (e.g., by telephone) may be made in a form reasonably calculated to reach the individual
    1. If there is insufficient or out-of-date contact information for ten (10) or more individuals, substitute notice shall:
        - be in the form of either a conspicuous posting for a period of ninety (90) days on the home page of The Company's website, or a conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and
        - include a toll-free phone number that remains active for at least ninety (90) days, where an individual can learn whether the individual's unsecured PHI may be included in the breach.
    2. Incapacitated Individuals. Written notice shall be made to the individual's personal representative
    3. Deceased Individuals: If The Company knows the individual is deceased and has the address of the next of kin or personal representative, written notice by first class mail may be made to either the next of kin or personal representative of the individual. Such notification may be made in one (1) or more mailings, as information becomes available. If the next of kin or personal representative's information is insufficient or out-of-date, precluding written notice, substitute notice need not be made
        - Urgent Notification Required. Where The Company deems notice urgent because of possible imminent misuse of unsecured PHI, The Company may provide information to affected individuals by telephone or other means, as appropriate, <u>in addition to written notice</u>

- Maintain a log or other documentation of such breaches and, no later than sixty (60) days after the end of each calendar year, shall provide notification to the Secretary of HHS of all breaches discovered during the preceding calendar year, by going to http://ocrnotifications.hhs.gov/ and filling out the form, as fully as possible

e. For a breach of unsecured PHI involving more than five hundred (500) residents of a state or jurisdiction, The Company shall:
   1. Notify the affected individual(s) within sixty (60) days

f. Breach notification shall be made through written notice, in plain language, and shall include the following, to the extent possible:
   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 covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches
   5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, website, or postal address

g. Notice shall be sent by first-class mail to the individual's last known address. or if the individual agrees to electronic notice (and such agreement has not been withdrawn), by electronic mail
   1. Insufficient or Out-of-Date Contact Information: If insufficient or out-of-date information precludes written notification, substitute notification (e.g., by telephone) may be made in a form reasonably calculated to reach the individual.
      - If there is insufficient or out-of-date contact information for ten (10) or more individuals, substitute notice shall:
        - be in the form of either a conspicuous posting for a period of ninety (90) days on the home page of The Company's website or a conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and
        - include a toll-free phone number that remains active for at least ninety (90) days where an individual can learn whether the individual's unsecured PHI may be included in the breach.
      - Incapacitated Individuals. Written notice shall be made to the individual's personal representative
      - Deceased Individuals: If The Company knows the individual is deceased and has the address of the next of kin or personal representative, written notice by first class mail may be made to either the next of kin or personal representative of the individual. Such notification may be made in one (1) or more mailings, as information becomes available. If the next of kin or personal representative's information is insufficient or out-of-date, precluding written notice, substitute notice need not be made

h. Urgent Notification Required. Where The Company deems notice urgent because of possible imminent misuse of unsecured PHI, The Company may provide information to affected individuals by telephone or other means, as appropriate, in addition to written notice.
    1. Notify prominent local media outlets serving the state or jurisdiction without unreasonable delay and in no case later than sixty (60) calendar days after discovery or a breach
i. Notification to the media shall include the following, to the extent possible:
    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 covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches
    5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, website, or postal address
        - Notify the Secretary of the Department of Health and Human Services (HHS) contemporaneously with notice to the affected individuals, by going to http://ocrnotifications.hhs.gov/ and filling out the form, as fully as possible

5). *Delay of Notification for Law Enforcement:* If a law enforcement official tells The Company that a required notification, notice, or posting would impede a criminal investigation or cause damage to national security, The Company shall:
a. if the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or
b. if the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily, but no longer than thirty (30) days from the date of the oral statement, unless a written statement is submitted by law enforcement during that time.

L. DISCIPLINARY STANDARDS FOR HIPAA PRIVACY VIOLATION

1). *Overview:* The Company has established a disciplinary policy and corresponding procedures for when the Health Insurance Portability and Accountability Act (HIPAA) Privacy Program policies and procedures are suspected of being violated. Adherence to applicable laws, rules, and regulations as well as The Company's Privacy Program is mandatory. Failing to report suspected noncompliance, participating in noncompliant behavior, or encouraging, directing, facilitating, or permitting, either actively or passively, noncompliant behavior may result in disciplinary action, up to and including termination. Also, if The Company learns that an individual knowingly fabricated, distorted, exaggerated, or minimized a report of misconduct, either to injure someone else or to protect himself or herself, the individual will be subject to disciplinary action, up to and including termination. (Link to WP 2.9 *Disciplinary Standards*).

2). *Implementation:* Anyone can file a complaint (refer to the Policies and Procedures for Privacy and Security Complaints). The Privacy Officer/Information Security Manager, or his or her designee, will process all privacy and security complaints.

If the Privacy Officer, or designee, determines per the Complaint process that there are violations of The Company policies and procedures, members of the workforce are to be disciplined. The discipline will be based on the severity and the number of times the same policy and procedure has been violated, consistent with The Company's Human Resource policies. The *Disciplinary Standards Policy* identifies examples of infractions and their corresponding disciplinary actions that apply to The Company's Privacy Program. The Company will impose the disciplinary actions identified beside the respective infractions. The disciplinary actions are listed as guidelines to be considered in determining the disciplinary action to be taken in response to infractions. The Company, in its sole discretion, may impose discipline less or more stringent than that called for by these guidelines, as set forth in the disciplinary protocol established under the Privacy Program

3). Non-Intimidation and Non-Retaliation: The Company has a policy of non-intimidation and non-retaliation for good faith participation in the Privacy Program, including but not limited to reporting potential issues, investigating issues, self-evaluations, audits and remedial actions, and reporting to appropriate officials. (Link to WM 2.9 *Disciplinary Standards, Section C, Non-Retaliation and Non-Retribution)*

Reference Appendix PP 2.1 D- *Discipline for HIPAA Privacy Violation Log*.

M. PRIVACY EDUCATION AND TRAINING

1.) *Overview:* All Company employees are responsible for ensuring that protected health information is used and disclosed appropriately. Company employees means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for The Company, is under the direct control of The Company, whether or not they are paid by The Company. The Company ensures that employees are effectively trained about The Company's Privacy Program and other relevant policies, specific regulatory compliance issues, and their responsibilities.

2). *Implementation:* The Company maintains an ongoing privacy training program, which includes:

a. Our Privacy Program - For existing members of the workforce:
    1. Training must be completed as expeditiously as possible
    2. Training must be completed within sixty (60) days if their functions are affected by a material change in the policies and procedures
b. Checklist Orientation, including Privacy-specific education - During new hire orientation, all new hires, regardless of position and seniority, are trained on the Privacy Program and specific requirements and expectations under the program. For a new member of the workforce, training must be completed within thirty (30) days after the person joins the workforce
c. Regular Privacy Training

The Company's training and education program is designed to communicate The Company's Privacy Program standards and procedures to employees in a meaningful and effective manner, and to ensure consistent application of the Program's policies. The Company training program is geared to the level of responsibility and job function.

Training sessions utilize classroom, lecture, recorded instruction, and/or other means of communication, as appropriate, to accommodate the skills, experience, and knowledge of the trainees. Other forms of education are employed, including the use of posters, bulletin boards, paycheck stuffers, etc., to inform employees of new privacy issues or to reinforce aspects of past training. No matter how the information is presented, the training is documented, including the date, attendees, and agenda.

It is the Privacy Officer's responsibility to establish and coordinate training activities, and to maintain a library of privacy-related information and training materials. Human Resources administers the training program.

All privacy trainings are mandatory.

N. CONFIDENTIAL INFORMATION TRAINING

1). *Overview:* All employees and volunteers are required to participate in The Company's confidentiality training program. All employees and volunteers are required to sign a *Confidential Information Agreement*.

2). *Procedure:* Confidentiality training will be provided to new hires during orientation. Employees and volunteers are required to attend review sessions annually. Topics to be covered in training include:

1. The responsibility of employees to maintain privacy of residents
2. Company's policies regarding the release of private information
3. Consequences for breach of privacy/confidentiality

Additional training may be provided to employees who deal directly with the distribution of private information.

1. A *Confidential Information Agreement* must be signed by all employees and volunteers following their initial training session
2. Agreements will be stored in employee's personnel files
3. Employees may be re-trained following changes to the above policy and/or procedures