Inteli-Care, LLC (IC) is committed to protecting the privacy and confidentiality of Protected Health Information (PHI) as required by the Health Insurance Portability and Accountability Act (HIPAA). This policy outlines the guidelines for employees to handle PHI in the course of their employment at IC. This policy establishes procedures for the handling and protection of PHI by all IC employees.

Role	Responsibility
Management	Responsible for ensuring employees understand the guidelines regarding the handling of PHI to keep private and confidential.
IC Employee	Responsible for adhering to all policies and procedures.
Human Resources	Assist with the notification and documentation process completed by the Management. Responsible for approving written documentation to ensure consistency.

Protected Health Information (PHI) refers to any individually identifiable health information received by the company's group health plans or received by a health care provider, health plan, or health care clearinghouse that relates to the past, present, or future health of an individual or the payment for health care. PHI includes information such as:

- Medical conditions
- Health status
- Claims experience
- Medical histories
- Physical examinations
- Genetic information
- Evidence of disability

As an employer that may maintain employee health records, IC is subject to HIPAA regulations. HIPAA establishes standards to safeguard PHI and applies to: Health Plans, Health care clearinghouses, Health care providers that conduct certain health care transactions electronically, and Business Associates of the above entities. All employees must safeguard the confidentiality, integrity, and availability of all PHI, including both paper and electronic forms (ePHI).

Privacy Rule: The HIPAA Privacy Rule protects the privacy of patient PHI while allowing for the necessary exchange of information for patient care. Key patient rights under the Privacy Rule include: the right to examine and obtain copies of their medical records, the right to request corrections to their medical records, and the right to restrict access to certain parts of their health information. The Privacy Rule protects PHI in any form, including electronic, paper, and verbal formats. This includes information such as:

- Common identifiers (name, address, birth date, Social Security Number)
- The patient's past, present, or future physical or mental health condition
- Health care provided to the patient

The Privacy Rule requires IC to:

- Notify patients of their privacy rights and how their information may be used.
- Adopt and implement appropriate privacy procedures.
- Train employees on privacy procedures.
- Secure patient records containing PHI to prevent unauthorized access.

Security Rule: The Security Rule mandates the protection of ePHI confidentiality, integrity, and availability. This applies to all Covered Entities, their Business Associates, and any organization that handles ePHI. All employees are responsible for safeguarding the confidentiality, integrity, and availability of all PHI, regardless of format (paper or electronic).

Breach Notification Rule: When a breach of PHI occurs, employees must promptly notify their manager. A breach is considered an unpermitted use or disclosure of PHI that compromises the security or privacy of the information.

- Factors considered in determining the severity of a breach include:
  - The nature and extent of the PHI involved.
  - The unauthorized person who used or acquired the PHI.
  - Whether the PHI was acquired or viewed.
- Notification of most breaches to authorities is required within 60 days of discovery, with no unreasonable delay.

Personnel records and disclosures of PHI will be maintained for a minimum of six years as required by federal law or for a longer period as required by state law. Records will be destroyed securely to prevent future compromise.