Langslide

Guidelines on Uses and Disclosure of Protected Health Information (PHI)

Version 1.0

SCOPE

This policy applies to the Employees in the designated Rudramsa Systems Pvt. Ltd.(hereinafter referred to as Organization, Company, etc). HIPAA Covered, Healthcare Components, and HIPAA Affected Areas, anyone rendering services as a Business Associate, and anyone who creates, receives, maintains, or transmits Protected Health Information (PHI) in any capacity.

PURPOSE

This document outlines the guidelines for properly and adequately using and disclosing information (PHI) in compliance with applicable laws, including the Health Insurance Portability and Accountability Act (HIPAA). These guidelines ensure the confidentiality of individuals' health information integrity and closure: Release, transfer, provisions of, access to, or divulgence in any manner of information outside the entity holding the information.

DEFINITIONS

- **Individually Identifiable Health Information (IIHI):** A subset of health information, including demographic information collected from an individual, and ① is created or received by a health care provider, health plan, employer, or health care clearinghouse; and ② relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual.
- **Protected Health Information (PHI):** Individually identifiable health information held or transmitted by a covered entity or its business associate in any form or medium, whether electronic, on paper, or oral.
- **Use:** Concerning individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis within an entity that maintains such information.
- **Covered Entity:** Healthcare providers, health plans, and healthcare clearinghouses that transmit PHI electronically.
- **Business Associate:** Any person or entity that performs services involving the use or disclosure of PHI on behalf of a covered entity.

ROLES & RESPONSIBILITIES

The Privacy Officer is responsible for ensuring appropriate security measures regarding PHI Data are taken.

POLICY

Permitted Uses and Disclosures of PHI: PHI may only be used or disclosed under the following circumstances:

- **For Treatment:**
    - PHI can be shared among healthcare providers to coordinate and manage a patient's care, such as sharing test results with a specialist.
- **For Payment:**
    - PHI can be disclosed to facilitate billing and payment activities, including processing claims and determining benefits eligibility.
- **For Healthcare Operations:**
    - PHI can be used for administrative, legal, and quality improvement activities, such as training healthcare staff or conducting audits.
- **With Authorization:**
    - Uses and disclosures of PHI for purposes outside of treatment, payment, or operations require explicit written authorization from the individual.
- **For Public Interest and Legal Requirements:**
    - PHI can be disclosed without authorization for purposes such as:
    - Public health activities (e.g., reporting communicable diseases).
    - Reporting abuse, neglect, or domestic violence.
    - Responding to legal proceedings or law enforcement requests.
    - Compliance with regulatory oversight.

Minimum Necessary Standard: When using, disclosing, or requesting PHI, reasonable efforts must be made to limit the information to the minimum necessary to accomplish the intended purpose.

Individual Rights: Individuals have the following rights concerning their PHI:

- **Right to Access:**
    - Individuals can access and obtain a copy of their PHI upon request.
- **Right to Request Amendments:**
    - Individuals can request corrections to their PHI if they believe it is inaccurate or incomplete.
- **Right to an Accounting of Disclosures:**
    - Individuals can request a record of certain disclosures of their PHI.
- **Right to Request Restrictions:**
    - Individuals can request restrictions on the use or disclosure of their PHI.

- **Right to Confidential Communications:**
    - Individuals can request that communications regarding their PHI be sent to a specific location or method.

Safeguards for PHI: To protect PHI, the following safeguards must be implemented:

- **Administrative Safeguards:**
    - Staff training on privacy policies.
    - Designation of a Privacy Officer responsible for compliance.
- **Physical Safeguards:**
    - Secure storage of physical records.
    - Access controls to facilities containing PHI.
- **Technical Safeguards:**
    - Encryption of electronic PHI (ePHI).
    - Regular monitoring of system activity.
    - Use of secure passwords and authentication protocols.

Breach Notification: In the event of a breach of unsecured PHI, affected individuals, the U.S. Department of Health and Human Services (HHS), and, in some cases, the media must be notified without unreasonable delay and no later than 60 days after discovery of the breach.

Penalties for Non-Compliance: Failure to comply with PHI guidelines may result in:

- Civil monetary penalties.
- Criminal penalties, including fines and imprisonment.
- Reputational damage and loss of trust.

Training and Awareness: All workforce members with access to PHI must complete privacy training upon hire and periodically thereafter. Training should include:

- Understanding HIPAA requirements.
- Recognizing and reporting potential breaches.
- Safeguarding PHI in daily operations.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Mar 14 2026	Initial Release	Pronoy	Kartikeya	Kartikeya