Langslide

HIPAA Internal Privacy Policy

Version 1.0

PURPOSE

This Internal Privacy Policy is established to ensure the protection, confidentiality, and integrity of protected health information (PHI) as required by the Health Insurance Portability and Accountability Act (HIPAA).

SCOPE

This policy applies to all employees, contractors, volunteers, interns, and third-party vendors who have access to PHI in Rudramsa Systems Pvt. Ltd. (Hereafter referred to as "Organization, Company, etc). All workforce members must adhere to this policy to protect the privacy and security of individuals' health information.

DEFINITIONS

- **Protected Health Information (PHI):** Individually identifiable health information transmitted or maintained in any form or medium.
- **Covered Entities:** The organization is a covered entity under HIPAA.
- **Business Associates:** Any third-party service provider or entity that may have access to PHI.
- **Workforce Members:** Employees, contractors, volunteers, and interns who perform tasks on behalf of the Organization.
- **Minimum Necessary Standard:** The principle of accessing, using, or disclosing only the minimum amount of PHI necessary to accomplish a specific purpose.

ROLES AND RESPONSIBILITIES

The Privacy Officer, designated by the organization, oversees the development, implementation, and maintenance of HIPAA policies and procedures.

POLICY

Privacy Officer

The Organization will designate a Privacy Officer responsible for:

- Developing and implementing privacy policies and procedures.
- Conducting training on HIPAA compliance.
- Investigating and addressing privacy incidents.
- Monitoring compliance and performing risk assessments.

Permitted Uses and Disclosures of PHI

PHI may only be used or disclosed for:

- Treatment, payment, and healthcare operations.
- Compliance with legal requirements (e.g., public health reporting, law enforcement requests).
- Any other purpose with the individual's written authorization.

Minimum Necessary Standard

Workforce members must limit access to and disclosure of PHI to the minimum necessary to perform their job duties. Access controls and monitoring will be implemented to enforce this standard.

Safeguards for Protecting PHI

The Organization will implement administrative, physical, and technical safeguards, including:

- Administrative: Policies, training, and audits.
- Physical: Secure office spaces, locked file cabinets, and restricted areas.
- Technical: Encryption, firewalls, and secure user authentication.

Training and Awareness

All workforce members will receive HIPAA training during onboarding and annually thereafter. Training will include:

- Overview of HIPAA requirements.
- Identifying and reporting breaches.
- Proper handling of PHI.

Incident Reporting and Breach Notification

All suspected or actual privacy incidents must be reported immediately to the Privacy Officer. In the event of a breach:

- The Privacy Officer will investigate and document the incident.
- Affected individuals will be notified within 60 days if the breach meets HIPAA notification criteria.
- If applicable, reports will be filed with the U.S. Department of Health and Human Services (HHS).

Access and Amendment Rights

Individuals have the right to:

- Access their PHI upon request.
- Request corrections to their PHI if inaccuracies are identified.

Sanctions for Non-Compliance

Workforce members who fail to comply with this policy may face disciplinary action, up to and including termination of employment or contract.

Retention of Records

All records, including privacy policies, training materials, and breach investigations, will be retained for at least six years in compliance with HIPAA regulations.

SANCTIONS

Violations of this policy may result in disciplinary action, up to and including termination, by applicable policies and procedures.

REVIEW AND REVISION

This policy will be reviewed and updated to reflect changes in regulations, technology, and the organization's business processes.

REPORTING

Any suspected or actual breaches of PHI or violations of this policy must be reported to the Privacy Officer immediately.

CONTACT INFORMATION

For questions or concerns, contact Data Protection Officer (DPO)

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