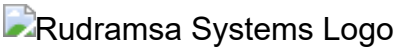

Rudramsa Systems

PHI De-identification Policy and Procedure

Version 1.0

PURPOSE

This policy aims and requirements for de-identifying PHI to protect individual privacy while enabling the lawful use of health information for secondary purposes such as research, quality improvement, and operational analysis.

SCOPE

This policy applies to all workforce members, contractors, business associates, and other entities handling PHI under Rudramsa Systems Pvt. Ltd. (Herein after referred as “Organization”, “Company etc)”. It governs all activities involving the de-identification of PHI by HIPAA Privacy Rule (45 CFR §164.502(d) and §164.514(a)-(b)).

DEFINITIONS

Protected Health Information (PHI)

PHI includes any information that relates to an individual’s health status, provision of healthcare, or payment for healthcare that can be linked to an individual.

De-identified Data

Data that has been processed to remove or obscure identifying elements, ensuring that it cannot reasonably be used to identify an individual.

Identifiers

Under HIPAA, PHI is considered de-identified when the following 18 identifiers are removed or masked:

- Names
- All geographic subdivisions smaller than a state (e.g., street address, city, ZIP code)
- All elements of dates (except year) related to an individual (e.g., birth date, admission date, discharge date)
- Telephone numbers
- Fax numbers
- Email addresses

- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plates
- Device identifiers and serial numbers
- Web URLs
- IP addresses
- Biometric identifiers (e.g., fingerprints, voiceprints)
- Full-face photographs and comparable images
- Any other unique identifying number, characteristic, or code.

RESPONSIBILITIES

1. **Department/Unit Possession:** The department or unit possessing the PHI is responsible for implementing the de-identification process by this policy.
2. **Privacy Officer:** The Privacy Officer provides guidance, training, and oversight to ensure consistent and compliant implementation of the de-identification process across all departments.

DE-IDENTIFICATION METHODS

We use the following methods to de-identify PHI by HIPAA and industry best practices:

Safe Harbor Method

Under the Safe Harbor method, all 18 identifiers listed above are removed or masked, and no knowledge exists that the remaining data could be used to identify the individual.

Expert Determination Method

Based on analysis, an expert with appropriate statistical and scientific knowledge determines that the risk of re-identification is minimal. The expert must document:

1. The methods used to de-identify the data.
2. The results of their analysis.
3. Any mitigating steps are taken to reduce re-identification risk further.

PROCEDURES FOR DE-IDENTIFICATION

Identifying Data for De-identification

1. Identify datasets that contain PHI and require de-identification.
2. Assess the intended use of the de-identified data to determine the appropriate de-identification method.

Applying De-identification Methods

1. Remove all identifiers outlined in Section 5.1 for the Safe Harbor method.
2. For the Expert Determination method, engage a qualified expert to perform risk analysis and ensure proper documentation.

Verification of De-identification

1. Verify that all identifiers have been removed or masked.
2. Confirm that no reasonable basis exists to believe the information can be used to identify an individual.

Documentation Requirements

1. Maintain records of the de-identification process, including the method used, datasets affected, and expert determination (if applicable).
2. Retain documentation for a minimum of six years or as required by law.

RE-IDENTIFICATION PROHIBITION

Under no circumstances may de-identified data be re-identified without explicit authorization and a valid legal or operational purpose. Unauthorized re-identification will be subject to disciplinary action and potential legal penalties.

ROLES AND RESPONSIBILITIES

Workforce Members

1. Ensure PHI is de-identified according to this policy before using it for secondary purposes.
2. Report any issues or potential breaches immediately to the Privacy Officer.

Privacy Officer

1. Oversee the implementation and compliance with this policy.
2. Provide training and resources on de-identification practices.
3. Approve the use of expert determination methods and ensure proper documentation.

IT/Data Security Team

1. Implement technical safeguards to prevent unauthorized access to PHI and de-identified data.
2. Support de-identification through encryption, access controls, and anonymization tools.

USE OF DE-IDENTIFIED DATA

De-identified data may be used for the following purposes without additional consent:

1. Research and development.
2. Public health reporting.
3. Quality assurance and improvement.
4. Statistical analysis and trend forecasting.

MONITORING AND AUDITING

Regular audits will be conducted to ensure compliance with this policy. Audits will include:

1. Review of de-identified datasets.
2. Verification of de-identification procedures.
3. Assessment of safeguards to prevent re-identification.

TRAINING

All workforce members handling PHI must complete training on de-identification methods and this policy annually or as part of onboarding.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Feb 6 2026	Initial Release	Pronoy	Kartikeya	Kartikeya