Langslide

HIPAA Plan

Version 1.0

INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict Rudramsa Systems Pvt. Ltd. (herein referred to as the Organization, company, etc.)—ability to use and disclose protected health information (PHI).

Protected health information means information that is created or received by the Company and relates to the past, present, or future physical or mental health condition of a Patient/Client ("Participant"); the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant. It includes any data that identifies the participants or could reasonably be used to identify them. This applies to both living and deceased individuals. Protected health information includes information about persons living or deceased.

Some examples of PHI are:

- Participant's medical record number
- Participant's demographic information (e.g., address, telephone number)
- A participant's medical record includes information from doctors, nurses, and other healthcare providers.
- Images of the participant
- Conversations a provider has about a participant's care or treatment with nurses and others
- Information about a participant in a provider's computer system or a health insurer's computer system
- Billing information about a participant at a clinic
- Any health information that can lead to the identification of an individual or the contents of the information can be used to make a reasonable assumption about the individual's identity.

It is the Company's policy to comply fully with HIPAA requirements. To that end, all staff members who have access to PHI must comply with this HIPAA Privacy and Security Plan. For purposes of this plan and the Company's use and disclosure procedures, the workforce includes individuals who would be considered part of the workforce under HIPAA, such as employees, interns, board members, and other persons whose work performance is under the organization's direct control. "Employee" or "staff member" includes all these types of workers.

No third-party rights (including but not limited to the rights of participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Plan. The organization reserves the right to amend or change this Plan at any time (and even retroactively) without notice.

All staff must comply with HIPAA privacy and information security policies. If, after an investigation, you are found to have violated the organization's HIPAA privacy and information security policies, you will be subject to disciplinary action up to termination or legal ramifications if the infraction requires it.

RESPONSIBILITIES AS COVERED ENTITY

- **Data Protection Officer (DPO) (hereinafter referred to as Privacy Officer)**

  The Privacy Officer will be responsible for developing and implementing policies and procedures relating to privacy, including but not limited to this Privacy Policy and the Company's use and disclosure procedures. The Privacy Officer will also serve as the contact person for participants who have questions, concerns, or complaints about the privacy of their PHI. The Privacy Officer can be reached at pronoy@langslide.com

- **Incident Response Team**

The Privacy Officer investigates the Incident Response, and the result of the investigation is shared with the CEO and Top Management. If a security incident results in a wrongful disclosure of PHI, the Privacy Officer, in conjunction with the Incident Response Team, will take appropriate actions to prevent further inappropriate disclosures. In addition, Human Resources and Legal may be consulted as part of the review team to assist in reviewing and investigating privacy incidents when required. Suppose the Privacy Officer and Incident Response Team have not resolved the incident. In that case, the Privacy Officer shall involve anyone determined to be necessary to assist in resolving the incident. If participants need to be notified of any lost/stolen PHI, the Privacy Officer will send PHI Theft/Loss Disclosure Letters to all possible affected individuals.

- **Workforce Training**

The Company's policy is to train all members of its workforce who have access to PHI on its privacy policies and procedures. All staff members receive HIPAA training. Whenever a privacy incident occurs, the Privacy Officer, in collaboration with management, will evaluate the occurrence to determine whether or not additional staff training is required. Depending upon the situation, the Privacy Officer may determine that all staff should receive training specific to the privacy incident.

The Privacy Officer will review any privacy training developed as part of a privacy incident resolution to ensure the materials adequately address the circumstances regarding the privacy incident and reinforce the Company's privacy policies and procedures.

- **Safeguards**

The Company has established technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Technical safeguards include limiting access to information by creating computer firewalls. Physical safeguards include locking doors or filing cabinets and periodically changing biometric passwords. Additionally, all staff members can only access PHI using their login information. Projects where PHI is captured or processed are physically separated from the other office areas, and a separate biometric device shall be available to access such areas.

Firewalls ensure that only authorized employees have access to PHI, that they have access to only the minimum amount necessary for their job functions, and that they will not further use or disclose PHI in violation of HIPAA's privacy rules.

- **Data Storage / Backup**

All data in the local data center is backed up using a backup tool, i.e., industry-standard secure backup procedures with AES 256. The organization currently utilizes technology that allows the IT team to quickly remove, disable, and enable staff members access to PHI.

- **Privacy Notice**

The Privacy Officer is responsible for developing and maintaining a notice of the Company's privacy practices that describes:

  - The uses and disclosures of PHI that the Company may make
  - The individual's rights; and
  - The Company's legal duties concerning the PHI
  - On an ongoing basis, at the time of an individual's enrollment into the Company

The privacy notice will inform participants that the Company will have access to PHI. It will also describe the Company's complaint procedures, the name and telephone number of the contact person for further information, and the date of the notice.

The notice of privacy practices will be individually delivered to all participants.

- **Complaints**

  The Privacy Officer will be the Company's contact person for receiving complaints. The Privacy Officer is responsible for creating a process for individuals to lodge complaints about the Company's privacy procedures and a system for handling such complaints. Upon request, a copy of the complaint form shall be provided to any participant.

- **Disciplinary Action for Violations of Privacy Policy**

  Disciplinary action, up to and including termination, will be taken for using or disclosing PHI in violation of this HIPAA Privacy Plan. The organization's disciplinary policy covers everything in detail.

- **Mitigation of Inadvertent Disclosures of Protected Health Information**

  To the greatest extent possible, the organization shall mitigate any harmful effects that become known to it because of the use or disclosure of the Participant's PHI, which violates the policies and procedures outlined in this Plan. As a result, if an employee becomes aware of a disclosure of protected health information, either by a staff member of the Company or an outside consultant/contractor that is not in compliance with this Policy, immediately contact the Privacy Officer so that the appropriate steps to mitigate the harm to the participant can be taken.

- **No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy**

  No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA.

- **Plan Document**

  The Plan document includes provisions to describe the permitted and required uses and disclosures of PHI. Specifically, the Plan document requires the organization to:

  - Not use or further disclose PHI other than as permitted by the Plan documents or as required by law
  - Ensure that any agents or subcontractors to whom it provides PHI received from the Company agree to the same restrictions and conditions that apply to the organization
  - Report to the Privacy Officer any use or disclosure of the information that is inconsistent with the permitted uses or disclosures.
  - Make PHI available to participants, consider their amendments, and, upon request, provide them with an accounting of PHI disclosures.
  - Make the Company's internal practices and records relating to the use and disclosure of PHI received by the Company available to the Department of Health and Human Services (DHHS) upon request

- **Documentation**

  The Company's privacy policies and procedures shall be documented and maintained for at least six years. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements, and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented.

  If a change in law impacts the privacy notice, the privacy policy must be promptly revised and made available. Such a change is effective only when PHI is created or received after the effective date of the notice.

  The organization shall document certain events and actions (including authorizations, requests for information, and complaints) relating to an individual's privacy rights.

The documentation of any policies and procedures, actions, activities, and designations may be maintained in either written or electronic form.

- **Incident Report**

  The Company has developed a Security Incident Final Report form. This form documents reports of privacy breaches referred to the Privacy Officer by staff members who have reviewed or received the suspected incident.

  After receiving the Incident Report form from team members, the Privacy Officer classifies the incident and its severity and analyzes the situation. The company shall retain the documentation for a minimum of six years from the date of the reported incident.

  If the Privacy Officer can resolve the incident, the Privacy Officer shall also document the actions taken to resolve the issue in the Incident Report form.

- **Electronic Health Records**

  Electronic health records must comply with federal HIPAA laws. Unlike health records, electronic health federal HIPAA is encrypted — using technology that makes them unreadable to anyone other than an authorized user — and security access parameters are set so that only authorized individuals can view them. Further, EHRs offer the added security of an electronic tracking system that provides an accounting history of when records have been accessed and who accessed them.

- **Access Authorization**

  Organizations will grant access to PHI based on their job functions and responsibilities. The Privacy Officer, in collaboration with IT and senior management, is responsible for determining which individuals require access to PHI and what level of access they require through discussions with the individual's manager and/or department head.

USE AND DISCLOSURE OF PHI

- **Use and Disclosure Defined**

  The Company will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

  - Use: The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the Company or a Business Associate.
  - Disclosure: For information that is protected health information, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within the organization with a business need to know PHI.

- **Access to PHI Is Limited to Certain Employees**

  All staff who perform Participant functions directly on behalf of the Company or on behalf of group health plans will have access to PHI as determined by their department and job description and as granted by IT.

  These employees with access may use and disclose PHI as required under HIPAA. Still, the disclosure of PHI must be limited to the minimum amount necessary to perform the job function. Employees with access may not disclose PHI unless an approved, compliant authorization is in place or the disclosure otherwise is in compliance with this Plan and the use and disclosure procedures of HIPAA.

  Staff members may not access medical and/or demographic information for themselves, family members, friends, staff members, or other individuals for personal or other non-work-related purposes through our information systems or the participant's medical record, even if written or oral participant authorization has been given. If the staff member is a participant in the organization's plans, they must go through their Provider to request their own PHI.

In the very rare circumstance that a staff member's job requires him/her to access and/or copy the medical information of a family member, a staff member, or another personally known individual, he/she should immediately report the situation to his/her manager, who will determine whether to assign a different staff member to complete the task involving the specific Participant.

Your access to your own PHI must be based on the same procedures available to other participants, not based on your job-related access to our information systems. For example, suppose you are waiting for a lab result or want to view a clinic note or operative report. In that case, you must contact your physician for the information or make a written request to the Privacy Officer. You cannot access your information; you must go through all the appropriate channels as any participant would have to.

HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure.

The "minimum-necessary" standard does not apply to any of the following:

- Uses or disclosures made to the individual
- Uses or disclosures made under a valid authorization
- Disclosures made to the Department of Labor of the participant state
- Uses or disclosures required by law, and
- Uses or disclosures required to comply with HIPAA.

Minimum Necessary When Disclosing PHI. For making disclosures of PHI to any business associate or providers or for internal/external auditing purposes, only the minimum necessary amount of information will be disclosed.

All other disclosures must be reviewed individually by the Privacy Officer to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum Necessary When Requesting PHI. Only the minimum necessary amount of information will be requested when requesting disclosure of PHI from business associates, providers, or participants for claims payment/adjudication or internal/external auditing purposes.

All other requests must be reviewed individually by the Privacy Officer to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

Disclosure of PHI is limited to certain employees only; data in transit and at rest is encrypted by AES 256 encryption.

- **Disclosures of PHI to Business Associates**

With the Privacy Officer's approval and HIPAA compliance, employees may disclose PHI to the Company's business associates and allow the Company's business associates to create or receive PHI on its behalf. However, before doing so, the Company must obtain assurances from the business associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees must contact the Privacy Officer and verify that a business associate contract is in place.

Business Associate is an entity that:

- Performs or assists in performing a Company function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.), or
- Provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

Examples of Business Associates are:

- A third-party administrator that assists the Company with claims processing.

- A CPA firm whose accounting services to a health care provider involve access to protected health information.
- An attorney whose legal services involve access to protected health information. A consultant who performs utilization reviews for the company.
- A healthcare clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of the Company and forwards the processed transaction to a payer.
- An independent medical transcriptionist who provides transcription services for the Company. A pharmacy benefits manager who manages a health plan's pharmacist network.

- **Disclosures of De-Identified Information**

  The Company may freely use and disclose desidentified information. De-identified information is health information that does not identify an individual, and there is no reasonable basis to believe that it can be used to identify an individual. A covered entity can determine that information is de-identified in two ways: either by professional statistical analysis or by removing 19 specific identifiers.

  Nineteen specific elements listed below — relating to the participant, employee, relatives, or employer — must be removed, and you must ascertain whether there is no other available information that could be used alone or in combination to identify an individual.

  - Names
  - Geographic subdivisions smaller than a state
  - All elements of dates (except year) related to an individual — including dates of admission, discharge, birth, and death — and for persons >89 years old, the year of birth cannot be used.
  - Telephone number
  - Electronic mail addresses
  - Social Security Number
  - 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
  - Internet protocol addresses
  - Biometric identifiers, including finger and voiceprints
  - Full-face photos and comparable images
  - Any unique identifying number, characteristic, or code
  - Billing Details
  - Medical Prescriptions

A person with appropriate expertise must determine that the risk is very small and that the information could be used alone or in combination with other reasonably available information by an anticipated recipient to identify the individual. This person must document the methods and justification for this determination.

- **Removing PHI from Company Premises**

  When the organization deems it necessary for an employee to work from a location other than one of our sites, PHI may be accessed and/or removed under the following circumstances:

  - Before removing PHI from the organization for company business, you must receive approval from your Department Head.
  - The organization will only allow the removal of PHI from paper (participant records, reports) when transported in a secure lock box and approved by the Department Head and the Privacy Officer.
  - The organization will provide laptop computers for employees working offsite and access PHI in a non-organizational setting. Any files on these computers are saved to the network and, therefore, secure.
  - A staff member with progress notes and other forms that need to be signed by their supervisors can be brought back to the organization in a locked carrying case. These documents can also be saved on the organization server in a designated secure file on the company network or a password-protected flash drive received by IT.
  - The privacy officer may only approve the electronic removal of PHI (using removable media) to work from an organization setting in advance. In the very rare circumstance that it becomes necessary, the PHI should be rigorously safeguarded physically and electronically, including employee-performed encryption of all files. Most removable media can be assigned a password.

  The following safeguards are required of all employees when working from a non-organizational site:

  - Outside the facility, we only work on health information in a secure private environment.
  - Keep the information with you at all times while in transit.
  - Do not permit others to have access to the information.
  - Never email participant information.
  - Don't save participant information to your home computer.
  - Do not print records of any type.
  - Do not record login information on or near the computer.
  - Return all information the next business day or as soon as required.

  The organization will immediately investigate any incident involving the loss or theft of PHI taken off-site.

PARTICIPANT INDIVIDUAL RIGHTS

- **Access to PHI and Requests for Amendment**

  HIPAA gives participants the right to access and obtain copies of their PHI that the Company or its associates maintain. HIPAA also allows participants to request to have their PHI amended. The Company will provide access to PHI and consider requests for amendments submitted in writing by participants.

- **Accounting**

  An individual has the right to obtain an accounting of certain disclosures of their PHI. This right to accounting extends to disclosures made in the last six years, other than disclosures:

- To individuals about their own PHI
- Incident to an otherwise permitted use or disclosure or under authorization

The Privacy Officer is responsible for responding to a request for Accounting.

- **Requests for Alternative Communication Means or Locations**

  Participants may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, they may ask to be called only at work rather than at home. Such requests may be honored if, in the sole discretion of the organization, they are reasonable.

  However, the organization shall accommodate such a request if the participant provides information that disclosing all or part of that information could endanger the participant. In collaboration with managers, the Privacy Officer is responsible for administering requests for confidential communications.

- **Requests for Restrictions on Uses and Disclosures of PHI**

  A participant may request restrictions on using and disclosing the participant's PHI. It is the Company's policy to attempt to honor such requests if, in the sole discretion of the Company, the requests are reasonable. The Privacy Officer is responsible for processing requests for restrictions.

- **When a Participant Requests a Copy of their Record**

  Since the organization will be working as a Business Associate (providing Software solutions), no information will be given to any requestor.

- **Acceptable Methods of Verification of Identity for Release of PHI**

  Since the organization will be working as a Business Associate (providing business solutions), no information will be given to any requestor.

PHI BREACH REPORTING

This section addresses the Company's privacy requirements for reporting, documenting, and investigating a known or suspected action or adverse event resulting from unauthorized use or disclosure of individually identifiable health information.

A privacy breach is an adverse event or action that is unplanned, unusual, and unwanted and occurs as a result of non-compliance with the company's privacy policies and procedures. A privacy breach must pertain to the unauthorized use or disclosure of health information, including 'accidental disclosures' such as misdirected emails.

The Privacy Officer shall immediately investigate and attempt to resolve all reported suspected privacy breaches.

Staff members must verbally report to their supervisor any event or circumstance that is believed to be an inappropriate use or disclosure of a participant's PHI. If the supervisor is unavailable, the staff member must notify the Privacy Officer within 24 hours of the incident. If the manager determines that further review is required, the manager and staff member will consult with the Privacy Officer to determine whether the suspected incident warrants further investigation.

The Privacy Officer will document all privacy incidents and corrective actions taken. Documentation shall include a description of corrective actions, if any are necessary, an explanation of why corrective actions are unnecessary, and any mitigation undertaken for each specific privacy incident. All documentation of a privacy breach shall be maintained with the Privacy Officer and retained for at least six years from the date of investigation. Such documentation is not considered part of the participant's health record.

If the participant is unaware of a privacy incident, the Privacy Officer shall investigate the incident thoroughly before determining whether the participant should be informed. If the participant is aware of a privacy incident, the Privacy Officer

shall contact the participant within three business days of receiving notice of the incident. The method of contact is at the discretion of the Privacy Officer, but resulting communications with the participant must be documented in the incident report. In addition, any privacy incident that includes a disclosure for which accounting is required must be documented and entered into accounting.

Staff who fail to report known PHI/security incidents or fail to report them promptly may be subject to disciplinary action up to termination.

- **Breach Notification Requirements**

  Following a breach of unsecured protected health information, covered entities must notify affected individuals, if necessary and, in certain circumstances. In addition, business associates must notify covered entities of a breach.

  - **Individual Notice:**

    Covered entities must notify affected individuals after discovering unsecured protected health information breaches. Covered entities must provide this individual notice in written form or by e-mail if the affected individual has agreed to receive such notices electronically. Suppose the covered entity has insufficient or out-of-date contact information for ten or more individuals. In that case, the covered entity must provide substitute individual notice by either posting the notice on the homepage of its website or by giving the notice in significant print or broadcast media where the affected individuals likely reside. Suppose the covered entity has insufficient or out-of-date contact information for fewer than ten individuals. In that case, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

    These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the violation; the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the damage, and prevent further breaches, as well as contact information for the covered entity. Additionally, for substitute notice provided via web posting or significant print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach.

  - **Media Notice:**

    Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely notify appropriate media outlets serving the affected area through a press release. Like an individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach. It must include the same information required for the individual notice.

  - **Notice to the Secretary:**

    In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of Health and Human Services ("the Secretary") of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS website and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such violations annually. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

  - **Notification by a Business Associate:**

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the breach's discovery. The notice must be provided to the covered entity without unreasonable delay and no later than 60 days from the breach's discovery. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach and any information required to be provided by the covered entity in its notification to affected individuals.

- **Complaint/Concerns Reporting**

Concerns about the Company's privacy practices may arise in various contexts and may be received by many different persons at the Company. The Company must respond to concerns and complaints promptly. When a staff member hears or gets a complaint/concern, they should ask the complainant whether the complainant wishes to file a formal complaint and offer to assist the complainant with the form. Even if the person does not want to file a complaint or provide identifying information, the staff member should proceed with the following procedures.

Filing a Complaint

Participant's complaints of alleged privacy rights violations may be forwarded through multiple channels, such as telephone calls, letters via mail/email, or in person. If a staff member receives these complaints, the person receiving the complaint will:

- In response to a Telephone letter or In-Person request to File a Complaint – Complete the Privacy Complaint Form and immediately forward it to the Privacy Officer. Offer to forward a copy of the complaint form to the complainant.
- In response to a Letter or Email (printout) – Complete the Privacy Complaint Form and immediately forward it to the Privacy Officer. Attach the written complaint to the complaint form.
- In response to an Anonymous Complaint– Complete the Privacy Complaint Form based on the information provided and immediately forward it to the Privacy Officer. When possible, explain to the complainant that the Company must follow up on complaints whether or not they are anonymously filed.
- Team Members – Contact the Privacy Officer. Staff members may also complete the Privacy Complaint Form and forward it to the Privacy Officer. Upon receipt of a complaint, the Privacy Officer will initiate a primary investigation.
- Initial review – The Privacy Officer or their designee will review all complaints to determine if they allege a violation of established policies and procedures or other known regulations regarding the protection of individually identifiable health information. If there is no legitimate allegation, the Privacy Officer will, when possible, contact the Complainant by letter and inform them of this finding within 60 days. All documentation will be maintained as prescribed in this policy.
- Complaints requiring further review—If there is a legitimate allegation, the Privacy Officer or his/her designee will conduct a detailed investigation by reviewing the unit practices, contacting needed employees, working with the Security Officer (as applicable), and utilizing other resources as needed. Upon conclusion of the investigation, the Privacy Officer will, when possible, contact the Complainant by letter and inform him/her of the finding within 60 days.
- 60-day time frame—If this 60-day period cannot be met, the Privacy Officer shall, when possible, communicate this determination to the Complainant in writing and include an estimated timeframe for completion of the investigation.
- Outcome of Investigation—The investigation aims to determine whether the Company's policies and procedures comply with the privacy standards mandated by HIPAA. The Company will mitigate, to the extent practicable, any harmful effect that is known of the use or disclosure of PHI in violation of the Company's policies and procedures

or HIPAA's privacy requirements by the Company or any of its Business Associates. If disciplinary action is recommended, the Privacy Officer or their designee will coordinate any action with management.

- Documentation — All complaints sent to the Privacy Officer shall be documented in a format that includes all the information on the Privacy Complaint Form. The Privacy Officer will maintain all completed complaints' documentation for six years from the initial date of the complaint.

- **Non-Retaliation**

  The Company shall not intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against anyone who has reported a privacy incident.

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