Data Protection and Privacy Policy

Date	Version	Created/Modified By	Approved By	Change Description
20-Jul-21	1.0	Senthil Kumar	Rama	First Release
10-Aug-24	1.1	Subbaiya	Bala	Few new clauses
26-Aug-26	1.2	Jeevan	Bala	Google Health privacy updates

Purpose

The purpose of this document is to outline the policy of Innovation Minds and each of its direct and indirect subsidiaries regarding direct communications to the public and/or specific employees to ensure compliance with Standards for Privacy of Individually Identifiable Health Information.

Protect important records from loss, destruction, falsification and maintain privacy in accordance with statutory, regulatory, contractual and business requirements.

1. Scope

This policy applies to all employees of Innovation Minds and any of its subsidiaries. Human Resources and the Chief Executive Officer ("CEO") are responsible for working with the Board of Directors to ensure that the Privacy Protection policy is adhered to.

Policy Enforcement: All policy additions, modifications, and deletions are subject to review for appropriateness and approval by Innovation Minds' Privacy Officer, CTO and the Board of Directors.

Responsibility: The Director of Human Resource, Privacy Officer, and the CEO are responsible for the interpretation, administration, and enforcement of this policy.

This Privacy Policy is effective 10-Aug-24, and is the responsibility of the Privacy Officer, who may amend it, in any respect, as he or she deems necessary or appropriate from time to time with the approval of the Chief Operations Officer.

2. Principle

A number of countries have introduced legislation placing controls on the collection, processing and transmission of personal data. Depending on the respective national legislation controls may impose duties on those collecting, processing and disseminating personal information and restrict the ability to transfer that data to other countries. Data Protection and privacy is achieved by implementing controls specified by the national laws on data protection and privacy.

3. Policy

It is the policy of Innovation Minds to comply with the regulations stipulated in HIPAA, SB 168 and Civil Code section 1798.85(a). Innovation Minds' Privacy Protection policy includes physical information access, posted information, print, facsimiles, electronic communications, telephone exchanges, and mail.

This policy covers all Social Security Numbers, medical records and other individually identifiable health information held or disclosed by a covered entity, in any form, whether

communicated electronically, on paper, or orally.

Innovation Minds considers maintaining the security and confidentiality of Protected Health Information (PHI) and Social Security Numbers (SSN) a matter of its highest priority. Each person accessing Innovation Minds data and resources holds a position of trust relative to this information and must recognize the responsibilities entrusted in preserving the security and confidentiality of this information. The following conditions apply to all those having access to Protected Health Information and Social Security Numbers.

While Innovation Minds strives to hire employees of high integrity, Innovation Minds establishes policies, practices, and standards in order to comply with various federal and state regulations. Employees who engage in conduct that violates Company policies, practices, or standards or whose performance is unsatisfactory may be subject to corrective action (up to and including termination).

4. Standards

5.1 Physical Access Safeguards and Clean Desk Practices

a) **Posted Information**: Employees may not publicly post or display in any manner an individual's Social Security Number. This means that employees may not communicate or otherwise make available to the general public an individual's Social Security Number.

b) **Print:** A Responsible Employee must take reasonable steps to ensure that all print jobs containing PHI are retrieved and viewed only by a Responsible Employee. Employees may not print an individual's Social Security Number on any card, ID, or badge required for the individual to access products or services provided by the company.

c) **Facsimiles**: A responsible employee must take reasonable steps to ensure that all incoming faxes containing PHI are retrieved and viewed only by a Responsible Employee. In the course of performing ministerial tasks on behalf of our employer clients, Innovation Minds employees may need to send to third parties' information containing Social Security Number[s] for verification, enrollment, eligibility and administrative purposes. Employees may forward this information to third parties provided the purpose for which information containing Social Security Numbers[s] is clearly stated in the cover sheet always utilized in the transmission.

d) **Shredding of Printed Materials and Handwritten Notes**: Any Innovation Minds employee that provides services to a member must promptly shred, or store in a secure place until shredding is appropriate, any notes that contain a member's name, Social Security Number, benefits information, protected health information or any other applicable personal information.

e) **Computer Protocol**: All employees must lock their computer when stepping away from their desk.

f) **Secured Areas**: All Innovation Minds offices are considered "secured areas" and must be treated as such. Any visitor to an office must be greeted by the receptionist or employee on duty and will be issued a "Visitor" pass. All doors that open to the public are locked at all times and opened with an employee key card.

5.2 Electronic Communications

a) Emails and Data Files: Employees may not transmit or require an individual to transmit his or her Social Security Number over the Internet, unless the connection is secure, or the Social Security Number is encrypted. The use of password-protected documents is also acceptable, if the password is kept secure.

b) Internet Web Sites: Employees may not utilize or require an individual to utilize his or her Social Security Number to access an Internet Web site, unless a password or a unique personal identification number ("PIN") or another authentication device is also required to access the Web site.

5.3 Electronic Access to Member Information

a) Safeguards of Historic information: Access to this information is limited to select team. The information is accessible on a secured application and restricted to those with the correct user id and password.

b) CRM Usage and Safeguards: All member and/or client calls are documented on the Innovation Minds CRM system. The CRM system tracks the following information:

- Member
- Client
- Carrier
- Reason for call
- Topic of call
- Duration of call
- Status of call
- Resolution of call
- Innovation Minds employee taking call
- Any other pertinent information

c) Disclosure of Confidential Medical Information: Any electronic CRM file that contains protected health information will be indicated with a flag on the record to alert the Innovation Minds employee to request verbal confirmation of the member's identification or a written authorization to release information to a third party. When documenting such information into the CRM system an alert must be activated. Protected health information includes, but is not limited to the following:

- High Blood Pressure
- Heart, Liver and/or kidney disease
- Diabetes
- Mental Illness
- Prescription Medications

- HIV Testing Results
- Herpes or Hepatitis Diagnosis

Individual health information provided to an employer by or on behalf of an employee in connection with verifying an absence from employment, request for a reasonable accommodation of a disability, workers compensation claim, or other employment-related purpose, is not subject to this Privacy Policy.

5.4 Mail

Employees may not print an individual's Social Security Number on any materials that are mailed to the individual, unless state and federal law requires the Social Security Number to be on the document to be mailed. Notwithstanding this provision, check your department administrative and workflow procedures regarding the printing of Social Security Numbers on certain documents.

Mail addressed to a Health Plan (or known to relate to a Health Plan) and sent to Innovation Minds must be delivered to a responsible employee. Any other correspondence addressed to the Company that contains PHI must be forwarded to a responsible employee. Mail likely to contain PHI sent to a Business Associate shall be handled and processed in accordance with the guidelines established by the Business Associate to reasonably assure compliance with the Privacy Policy. Mail containing PHI should be handled and stored in accordance with the same general guidelines.

5. Procedures

6.1 Protected Health Information (PHI) and Social Security Number (SSN) Confidentiality

The following procedures must be followed to maintain client confidentiality:

a) Collect SSNs preferably only where required to do so by federal or state law.

b) When collecting PHI and/or SSNs is allowed, but not required, by law, do so only as reasonably necessary for the proper administration of lawful business activities.

c) If a unique personal identifier is needed, we will develop our own or work with the client to use their own identifiers as a substitute for the SSN.

6.2 Inform individuals when you request their SSNs

a) Whenever you collect PHI and/or SSNs as required or allowed by law, inform the individuals of the purpose of the collection, the intended use, and the consequences of not providing the number.

b) Any conversations with members or clients must be conducted in a tone that is professional and low to prevent them from being overheard by other Innovation Minds employees/visitors.

6.3 Elimination of public display of PHI and SSNs

a) Do not put PHI and/or SSNs on documents that are widely seen by others, such as identification cards, badges, timecards, employee rosters, bulletin board postings, and other materials.

b) Do not send documents containing SSNs on them through the mail, except on applications or forms or as allowed by your department's workflow procedures.

When sending applications, forms or other documents required by law to carry SSNs through the mail, place the SSN where it will not be revealed by an envelope window. Where possible, leave the SSN field on forms and applications blank and ask the individual to fill it in before returning the form or application.

d) Do not send PHI and/or SSNs by email unless the connection is secure or the PHI and/or SSN are encrypted.

e) Do not require an individual to send his or her PHI and/or SSN over the Internet or by email, unless the connection is secure or the PHI and/or SSN are encrypted.

f) Do not require individuals to use SSNs as passwords or codes for access to Internet web sites or other services.

6.4 Control access to PHI and/or SSNs

Innovation Minds limits access to records containing PHI and/or SSNs only to those who need to see the information and numbers for the performance of their duties. Protect records containing PHI and/or SSNs, including back-ups, during storage by encrypting the numbers in electronic records or storing records in locked cabinets. Do not store records containing PHI and/or SSNs on computers or other electronic devices that are not secured against unauthorized access. Avoid sharing PHI and/or SSNs with other companies or organizations except where required by law or authorized by the individual. If you do share PHI and/or SSNs with other companies or organizations, including contractors, use written agreements to protect their confidentiality.

Prohibit such third parties from re-disclosing SSNs, except as required by law. Require such third parties to use effective security controls on record systems containing SSNs. Hold such third parties accountable for compliance with the restrictions you impose, including monitoring or auditing their practices.

NOTE: If PHI and/or SSNs are disclosed inappropriately and the individuals whose PHI and/or SSNs were disclosed are put at risk of identity theft or other harm, promptly notify your manager or Compliance Officer immediately.

6.5 Employee Commitment

When handling confidential information, each employee is held responsible to:

a) Respect the privacy and rules governing the use of any information accessible through the computer system or network and only utilize information necessary for performance of employee's job.

b) Respect the ownership of proprietary software. For example, do not make unauthorized copies of such software for your own use, even when the software is not physically protected against copying.

c) Respect the finite capability of the systems, and limit use so as not to interfere unreasonably with the activity of other users.

d) Respect the procedures established to manage the use of the system.

e) Prevent unauthorized use of any information in files maintained, stored, or processed by Innovation Minds.

f) Do not seek personal benefit or permit others to benefit personally by any confidential information or use of equipment available through employee's work assignment.

g) Adhere to all stated policies; including but not limited to the Privacy Protection Policy and any specific departmental guidelines.

h) Do not operate any non-licensed software on any computer provided by Innovation Minds.

i) Do not exhibit or divulge the contents of any record or report except to fulfill a work assignment and in accordance with Innovation Minds policy.

j) Do not knowingly include or cause to be included in any record or report, a false, inaccurate, or misleading entry.

k) Do not remove PHI and/or SSNs from the office where it is kept except in the performance of employee's duties.

l) Understand that the information accessed through all Innovation Minds information systems contains sensitive and confidential patient/member care, business, financial and hospital employee information, which should only be disclosed to those, authorized to receive it.

m) Do not release any authentication code or device to anyone else or allow anyone else to access or alter information under employee's identity.

n) Do not utilize other employee's authentication code or device to access any Innovation Minds system.

o) Do not write user id and passwords on paper and leave unsecured.

p) Respect the confidentiality of any reports printed from any information system containing patient/member information and handle, store and dispose of these reports appropriately.

q) Do not divulge any information that identifies PHI and/or SSNs.

r) Understand that all access to the system will be monitored.

s) Sign the Privacy Protection Policy Acknowledgement.

6. Email usage and retention policy

This policy defines the acceptable use of the company's corporate e-mail system, and it applies to all uses of company owned e-mail accounts.

Email policy provides the organization to protect messages from unauthorized access, modification, or denial of service. The objective is achieved by adopting

- Spam Filters
- Monitoring mechanisms
- AV Protection
- File upload restrictions (Size, type)
- Address restrictions
- Disclaimer Notification
- Encryption mechanisms

7.1 Acceptable Uses of Company E-mail Accounts

The company provides e-mail accounts for business usage only. Every staff member has the responsibility to maintain and enhance the company's public image and to use the company's e-mail system in a responsible and productive manner that reflects well on the company.

7.2. Unacceptable Uses of Company E-mail Accounts

- Company e-mail accounts may not be used for transmitting, retrieving, viewing, or storage of any communications of a discriminatory or harassing nature or materials that are obscene or "X-rated."
- Harassment of any kind is prohibited.
- No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, or sexual preference shall be transmitted.
- No excessively abusive, profane, or offensive language is to be transmitted through the company's e-mail system.
- E-mail messages or attachments may also not be used for any purpose that is illegal or against company policy or contrary to the company's best interests.
- Solicitation of non-company business, or any use of the company e-mail system for personal gain, is prohibited.

7.3 Communications

- Each employee is responsible for the content of all text, audio, or images that they place or send over the company's e-mail system.
- All e-mails must contain the identity of the sender and may not represent the sender as someone else or someone from another company.
- Any messages or information sent by an employee to another individual outside of the company via an electronic network (e.g., blog, IM, bulletin board, online service, or Internet) are statements that reflect on the company. While some users include personal “disclaimers” in electronic messages, there is still a connection to the company, and the statements may legally be tied to the company.
- Therefore, we require that all communications sent by employees via the company's e-mail system comply with all company policies and not disclose any confidential or proprietary company information.

7.4 Privacy

- E-mails are not private. The company reserves the right to monitor e-mail content ensuring that the e-mail system is used for appropriate purposes.
- Also, no security is 100 percent hacker-proof; someone outside the company may intercept and read e-mail.
- Routing of e-mail is not without errors; someone other than the intended recipient may receive the e-mail.
- Do not send anything by e-mail that should not be placed on the company bulletin board.

7.5 Personal E-mail Accounts

- Accessing personal e-mail accounts is prohibited from company-owned computers, as they are a potential source of computer viruses.
- No company related communication is permitted using personal e-mail accounts, as the communication may be subject to the company’s communication retention policy.

7.6 Spam

Sending unwanted e-mail of any kind (spam) using a company e-mail account is prohibited.

7. 7 Copyright Issues

- Employees on the company's Internet system may not transmit copyrighted materials belonging to entities other than this company. Please note that non-adherence to this policy puts the company in serious legal jeopardy and opens the company up to significant lawsuits and public embarrassment.
- All employees obtaining access to other companies' or individuals' materials must

respect all copyrights and may not copy, retrieve, modify, or forward copyrighted materials, except with permission.

- Failure to observe copyright or license agreements may result in disciplinary action up to and including termination. If you have questions about any of these legal issues, please speak with your manager or IT department before proceeding.

7.8 Monitoring

- The company routinely monitors usage patterns in its Internet communications. The reasons for this monitoring include cost analysis, security, bandwidth allocation, and the general management of the company's gateway to the Internet.
- All messages created, sent, or retrieved over the company's Internet are the property of the company and should be considered public information. Notwithstanding comments above regarding our present intention not to monitor content, the company must reserve the right to access and monitor the content of all messages and files on the company's Internet system at any time in the future with or without notice.
- Employees should not assume electronic communications are totally private and should transmit highly confidential data in other ways. Electronic messages regarding sensitive matters should warn that such communications are not intended to be secure or confidential. This is just good business sense.

7.9 Retention

- Company communications of any kind typically needs to be retained as you would any other corporate document. Certain e-mail communications must follow the requirements established in Document Retention Policy depending on the subject or purpose of the e-mail.
- Please remember that e-mails deleted from your e-mail inbox are still saved on the company e-mail server

7.10 Confidentiality

Any e-mail message that is meant to be confidential must be labeled as such in the subject line. Forwarding of confidential messages requires the permission of the original sender. The corporate e- mail system will automatically attach a confidential message notification to all e-mails that are sent to addresses outside of the organization. Do not attach your own individual confidentially notice as this will be redundant and may be inconsistent with the official company message.

7.11 Violations

Any employee who abuses the privilege of company facilitated access to the e-mail(s) will be subject to corrective action up to and including termination. If necessary, the company also reserves the right to advise appropriate legal officials of any violations.

7. Access Control Policy

The purpose of this policy is to control access to organization's systems, applications, networks and information systems assets.

The policy applies to all corporate computers and devices that store corporate information. It applies to all users of the organization's network, using any device that has access to the network

The implementation of protection measures provides the organization with the capability to restrict the accidental or intentional unauthorized use of, or alteration to, information assets. Underlying the concept of access control is the need for the organization to embrace the following control principles:

- Defense in depth.
- Segregation of duties.
- Need to know.
- Compensating control / Dual Control.

The basic principle of access control is that access to information will be granted on a need to know or need to have basis, as per job functions.

Access controls must be applied to enforce a separation between software developers, software testers, system/security administrators, database administrators, computer operators, and end users.

In environments where this separation of function is not feasible, compensating controls must be used to manage and document these functions, including logging and audit trails to record the actions of administrators.

If an emergency fix must be made to production data, a higher level of access may be granted to a developer through an approval and authorization procedure. An audit trail must record granting and removal of the additional access.

Requests for access to information resources must be submitted to Internal IT helpdesk by the employee's project leader or Process Owners/delegates. Helpdesk will review the request, create the necessary user accounts, and forward the request to the appropriate application security administrator as needed for granting application specific access.

Any exceptions to this policy must be approved in advance by CISO

8. Antivirus Prevention Policy

The purpose of this policy is to prevent the infection of company computers, computer systems and other digital devices by computer viruses or malware and other malicious code. This policy is intended to prevent major damage and loss of information to hardware, applications and user data and to promote appropriate awareness.

The policy applies to all corporate computers and devices that store corporate information. It applies to all users of the organization's network, using any device that has access to the network.

Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses and logic bombs. User should be made aware of the dangers of malicious code. This is achieved by

- Installing Anti-Virus software
- Updating Patches
- Periodic scanning of networks and systems
- User Awareness

All corporate computers and devices that store corporate information and that at any time connect to the corporate network must have approved and supported anti-virus software correctly installed, configured, activated, and updated with the latest virus definitions.

Any devices infected with a virus or other malicious code (collectively referred to as "malware") must be immediately disconnected from the corporate network until the infection has been removed.

When an enterprise-wide malware attack is in progress, corporate IT helpdesk must notify all corporate users via the best available method. After such an attack has been identified, all storage devices must be scanned using the latest virus definitions available.

All systems are monitored every day to ensure the latest patches are available.

If a particular operating system or computing platform does not have anti-virus protection available, use of a device using such an operating system must be approved by CISO, who shall determine the operating procedures necessary to minimize the possibility of malware infecting the corporate network.

9. Network Policy

To ensure that users are only provide with access to the services that they have been specifically authorized to use.

The policy applies to all IT assets on Innovation Minds' network.

The network usage policy ensures that access to networks and network services are controlled by adopting the following mechanisms

- Access control
- Authorization procedures
- Maintaining access control lists
- Monitoring mechanism
- Configuring Alerts
- Segregating Networks

The basic principle of network access control is that access to information will be granted on a need to know or need to have basis, as per job functions.

Network controls must be applied to enforce a separation between software developers, software testers, system/security administrators, database administrators, computer operators, call center personnel and end users.

Access to assets in the network shall be monitored periodically. Requests for access to information resources must be submitted to Internal IT Help Desk by the employee's project leader or Process Owners/delegates. Network access shall be granted only after authorization

Access control lists on the network shall be maintained. Alerts shall be configured on the network equipment's that are critical.

Any exceptions to this policy must be approved by CISO.

10. Secure Development Policy

The purpose of this policy is to set rules that govern the development of software in the organization.

The policy applies to development and maintenance of application software developed in the organization.

Software developed and maintained must be free of vulnerabilities that may be exploited by threats such as hackers, hacking software. Developers and testers should be made aware of rules that govern development of secure software in the organization. This is achieved by:

- Adopting secure development practices
- Penetration and Vulnerability testing

- Restricting source code
- Development and maintenance of software adopt standard application development guidelines
- Developer access to source code is controlled and is need based
- Software developed shall be tested for vulnerability
- Any exceptions to this policy must be approved in advance by CISO.

11. Software Installation Policy

The policy applies to all corporate computers and devices that store corporate information. It applies to all users of the organization's network, using any device that has access to the network.

Software is governed by intellectual property rights (IPR) and specific licensing terms and conditions. Free wares are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses and logic bombs. User should be made aware of rules that govern installation of software on Organization's computers. This is achieved by:

- Restricting installation privileges
- Periodic scanning of networks and systems
- User Awareness
- Installation of licensed software, free ware on organization's computer systems/devices are carried out by authorized administrators.
- The organization maintains the list of authorized licensed software and freeware
- All corporate computers and devices that store corporate information and that at any time connect to the corporate network must have approved software.
- All systems are monitored on a periodic basis to ensure that authorized software is available in organization's systems.
- Any exceptions to this policy must be approved in advance by CISO.

12. Data Retention Policy

This policy is to ensure the most efficient and effective way of retaining information for operational or regulatory compliance needs

This policy applies to all type of information (Electronic / Physical Data) used by employees, clients, and others who associated with the organization.

Data retention will be authorized after appropriate review with the relevant functional heads and controls are put in place and that these comply with the organization's

security policy. The goals of this DRP are to:

- Retain important documents for reference and future use
- Delete documents that are no longer necessary for the proper functioning of Organization
- Organize important documents for efficient retrieval
- Ensure that every employee in the Organization know what documents should be retained, the length of their retention, means of storage, and when and how they should be destroyed.

13. Definitions

Business Associate: "Business Associate" shall mean, Innovation Minds and its subsidiaries, a person or entity, which performs or assists in the performance of a function or activity involving the use or disclosure of PHI from or on behalf of a Health Plan. Such functions or activities include claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, re-pricing, and other professional services. “Business Associate” will include all employees of the Business Associate who perform or assist in the performance of functions on behalf of a customer

Covered Entity: "Covered Entity" shall mean a health plan, a health care clearinghouse, or a Health Care Provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA.

Proprietary Information: shall mean information relating to Innovation Minds and its Clients that is not generally known to the public, including be not limited to information that relates to past, present, or future research and development, trade secrets, products and services, pricing, marketing, financial matters, or business affairs (including policies, procedures, plans, and methods or operation).

Protected Health Information (PHI): means individually identifiable health information that

(a) Relates to the past, present, or future physical or mental condition of an individual, provision of health care to an Individual, or payment for such health care

(b) Can either identify the Individual or there is a reasonable basis to believe the information can be used to identify the Individual

(c) Is received or created by or on behalf of a customer.

Electronic Transmissions includes transactions using all forms of electronic media. Such transactions include the transfer of information over the Internet (wide-open), Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, and private networks. Electronic

media includes magnetic tape, disk, or compact disc media. Telephone voice response and “fax back” (a request for information made via voice using a fax machine and requested information returned via that same machine as a fax) systems and facsimile transmissions are not included.

Privacy Officer: The person designated by Innovation Minds as responsible for implementing and updating the Privacy Policy and for carrying out the duties assigned to him or her under the Privacy Policy. Reference to the Privacy Officer includes any person(s) to whom the Privacy Officer has made an applicable delegation under this policy.

Responsible Employee: An employee of Innovation Minds whose duties

(a) Require that the employee have access to PHI for purposes of Innovation Minds Operations

(b) Make it likely that he or she will receive or have access to PHI. Any employee who receives PHI from, or on behalf of Innovation Minds, even though his or her duties do not (or are not expected to) include receiving PHI; will be treated as a Responsible Employee under the Privacy Policy.

14. Google Health API Data Privacy and Protection

Google Health Data Access

Innovation Minds provides voluntary employee wellness challenges designed to encourage participants to build and maintain healthy habits through goal-based wellness programs.

Users can connect Google Health to Innovation Minds only through the Innovation Minds mobile application. When a user voluntarily connects Google Health and provides consent through the Google authorization flow, Innovation Minds receives read-only access only to the Google Health data categories authorized by the user.

Innovation Minds currently requests only the minimum Google Health permissions required for supported challenge functionality. The authorized Google Health data may include:

- Activity and fitness information, including daily steps and calories burned, used for steps and calories-burned challenges.
- Sleep information, including recorded sleep duration, used for sleep-hours challenges.

Innovation Minds does not request Google Health access to health metrics and measurements or mindfulness data. Innovation Minds accesses Google Health data only after the user has provided explicit authorization. The requested permissions are read-only and are not used to create, modify, or delete information in the user's Google Health account.

Purpose and Use of Google Health Data

Innovation Minds uses authorized Google Health data solely to provide the wellness challenge functionality selected by the participant. After Google Health is connected through the mobile application, Innovation Minds performs a daily backend synchronization of the authorized data.

The backend evaluates the synchronized data against the requirements of the user's applicable wellness challenges. When the authorized Google Health data satisfies the configured challenge requirement, Innovation Minds automatically processes the eligible challenge claim on behalf of the user. Daily steps and applicable activity information may be used for steps or calories-burned challenges, and recorded sleep duration may be used for sleep-hours challenges.

The raw Google Health data is processed by Innovation Minds backend services for this challenge functionality and is not presented as a standalone Google Health data dashboard. After an eligible challenge is claimed, the user can view the resulting claimed challenge details together with the associated integrated wellness application information in both the Innovation Minds mobile application and web application.

Google Health data is used solely for this wellness challenge functionality. Innovation Minds does not use Google Health data for advertising, targeted advertising, unrelated profiling, credit decisions, or other unrelated purposes.

Sharing, Transfer, and Disclosure of Google Health Data

Innovation Minds does not sell Google Health data or transfer it to advertising platforms, data brokers, information resellers, or other third parties for advertising or unrelated commercial purposes.

Google Health data may only be shared, transferred, or disclosed where necessary to provide or support the user-authorized Innovation Minds wellness challenge functionality, maintain the security and integrity of Innovation Minds services, comply with applicable legal or regulatory requirements, or as otherwise permitted by applicable Google Health API policies.

Where authorized service providers or contractors process information on behalf of Innovation Minds, access is limited to what is necessary for the applicable service and is subject to appropriate confidentiality, privacy, and security obligations.

Google Health API Developer and User Data Policy

The use of information received from Google Health API and/or Developer Tools will adhere to the Google Health API Developer and User Data Policy, including the Limited Use requirements.

Data Protection and Security

Innovation Minds applies reasonable administrative, technical, and organizational safeguards designed to protect Google Health data and other sensitive user information against unauthorized or unlawful access, use, alteration, disclosure, destruction, or loss. These safeguards include secure transmission using encrypted network connections, access controls and authentication, restricted access based on business need, protection of stored sensitive information, security monitoring, secure development practices, and confidentiality and security requirements for authorized service providers.

Data Retention and Deletion

Innovation Minds retains Google Health data only for as long as reasonably necessary to provide the applicable wellness challenge functionality, fulfill the purpose for which the information was collected, or satisfy applicable legal, regulatory, security, and operational requirements. Information that is no longer required for these purposes will be deleted or otherwise handled in accordance with Innovation Minds' applicable data retention and deletion procedures.

User Choice and Consent

Connecting Google Health to Innovation Minds is voluntary. Users are informed that Innovation Minds requests read-only access to activity and fitness data and sleep data, and are informed how those data categories are used for applicable wellness challenges before granting authorization. Users may revoke their Google Health authorization. Revoking authorization prevents Innovation Minds from obtaining new Google Health data using the revoked authorization. Previously stored information will be handled according to Innovation Minds' applicable retention and deletion policies and applicable legal requirements.