



Privacy & Security Policy

Sm8rtHealth Limited Liability Partnership (referred to as "we," "our," or "us") provides a hosted service ("the Sm8rtHealth service") used in relation to the receiving, processing, and transmitting of applications for life, travel, and health insurance risk assessment. The Sm8rtHealth service is utilized by consumers, advisers, brokers, agents, insurers, booking agencies, and software platforms (referred to as "you" or "your").

Our Intent

We will always treat any information you provide with the utmost care and take all reasonable steps to protect your best interests.

Privacy

In handling your personal information, we comply with the New Zealand Privacy Act 2020 and the Australian Privacy Act 1988, including the Australian Privacy Principles (APPs). This ensures robust privacy practices and safeguards.

Information We Collect

When you use the Sm8rtHealth service, we may collect personal information, including but not limited to:

- Identity data such as your name, email address, and date of birth.
- Health and lifestyle-related information.
- Employment details and other relevant application data.

Purpose of Collection

Your health and financial data provided will only be used to facilitate the receiving, processing, and transmitting of your insurance risk. We provide a service to Insurers, and the data ownership belongs to them. We will only ever use the data for risk assessment and analytics.

Your Rights

Under the New Zealand Privacy Act and Australian Privacy Principles, you have the right to:

1. Access the health information we hold about you.
2. Request correction of any inaccuracies in your data.
3. Request deletion of your data where permissible by law.
4. Withdraw consent for the processing of your data.

To exercise these rights, contact us at support@Sm8rtHealth.com.



Data Retention Statement

- Never retain client private personal data or data that can identify a person unless absolutely necessary for risk assessment
 - Do not permit input fields that include personal information
 - Personal information acceptable includes Gender and DoB, Occupation and Income
 - Unacceptable are email addresses, names, addresses, cell phone, social security numbers, tax numbers and Id numbers, passports.
 - **All applications are purged after a maximum of 91 days.**
-

Privacy in Relation to AI

Sm8rtHealth may utilise Artificial Intelligence (AI) technologies to assist with insurance risk assessments. We ensure that:

1. **Transparency:** All AI systems used are clearly disclosed to our clients and operate under strict guidelines.
 2. **Data Anonymisation:** All personal data is redact using a 3rd Party Service before processed in SM8 private AI cloud.
 3. **Human Oversight:** AI-based risk assessment is reviewed by qualified personnel to ensure accuracy and appropriateness.
 4. **Security:** Data processed by AI is encrypted and purged in accordance with our Data Retention Statement.
-

Emails and Communications

We may communicate with you via email regarding the Sm8rtHealth service. We take reasonable steps to ensure these communications are secure. However, as email is not always a secure medium, we recommend caution when sharing sensitive information. You can opt out of non-essential communications by contacting us.

Security

We take reasonable steps to protect your information from misuse, loss, or unauthorized access, modification, or disclosure. These steps include:

- Encryption of data in transit using TLS protocols.
- Storage on Amazon Web Services (AWS), with strict access controls and monitoring.
- Regular security audits and vulnerability assessments.



Although we strive to protect your information, no method of transmission over the internet or electronic storage is completely secure. We cannot guarantee absolute security but are committed to maintaining industry best practices to mitigate risks.

Terms of Use

By using the Sm8rtHealth service, you agree to the following:

1. Your use of the service is subject to this Privacy & Security Policy, which you have read and understood.
 2. You are responsible for keeping your password confidential.
 3. You must immediately report any suspected fraudulent or unauthorised activity.
 4. We reserve the right to access, review, copy, delete, and disclose information stored on our systems as required to maintain service integrity.
 5. We reserve the right to inspect any files stored or transmitted via our systems for compliance with this policy.
-

Data Breach Notification

In the event of a data breach, we will:

1. Promptly assess the scope and impact of the breach.
 2. Notify affected users and relevant authorities as required by New Zealand law.
 3. Take immediate remedial actions to secure the system and prevent further breaches.
-

Contact Us

For questions or concerns about this policy, please contact:

Email: support@Sm8rtHealth.com

Physical Address: Campus 261, Building 730, 261 Morrin Road, St Johns, Auckland 1072, New Zealand.

Sm8rtHealth Limited Liability Partnership