

Our Privacy Policy

Purpose

This Privacy Policy details how we protect your privacy and how we comply with the requirements of the *Privacy Act 1998 (Cth)* and the 13 Australian Privacy Principles. This policy also describes:

- who we collect information from;
- the types of personal information collected and held by us;
- how this information is collected and held;
- the purposes for which your personal information is collected, held, used and disclosed;
- how you can gain access to your personal information and seek its correction;
- how you may complain or inquire about our collection, handling, use or disclosure of your personal information and how that complaint or inquiry will be handled; and
- whether we are likely to disclose your personal information to any overseas recipients.

Policy

Who do we collect personal information from?

In the course of providing our products and services Health Reimagined may collect personal information from clients, potential clients, job applicants, employees, consultants, contractors and sub-contractors.

What types of personal information do we collect?

In the course of providing products and services we may collect:

Personal Information including names, addresses and other contact details; dates of birth; and financial information.

Sensitive Information including government identifiers (such as your TFN), your nationality, country of birth, professional memberships, family court orders and criminal records.

Health Information (particularly in relation to client records) including medical records, disabilities, immunisation details and psychological reports.

How do we collect and hold your personal information?

How we collect personal information will largely be dependent upon whose information we are collecting. If it is reasonable and practical to do so, we collect personal information directly from you.

Where possible Health Reimagined has attempted to standardise the collection of personal information by using specifically designed forms (e.g. our Application Forms and Referral Forms). However given the nature of our operations we often also receive personal information by email, letters, notes, over the telephone, in face-to-face meetings and through financial transactions.

We may also collect personal information from other people or independent sources, however, we will only do so where it is not reasonable and practical to collect the information from you directly.

Sometimes we may be provided with your personal information without having sought it through our normal means of collection. We refer to this as "unsolicited information". Where we collect unsolicited information we will only hold, use and or disclose that information if we could otherwise do so had we collected it by normal means. If that unsolicited information could not have been collected by normal means then we will destroy, permanently delete or de-identify the information as appropriate.

How we use your personal information?

We only use personal information that is reasonably necessary for one or more of our functions or activities (the primary purpose) or for a related secondary purpose that would be reasonably expected by you, or to which you have consented.

It may be necessary for Health Reimagined to disclose your personal information to certain third parties in order to assist us with one or more of our functions or activities. This may include organisations providing primary health care and associated services under an arrangement with us.

We only collect sensitive information reasonably necessary for one or more of these functions or activities if we have the consent of the individuals to whom the sensitive information relates, or if the collection is necessary to lessen or prevent a serious threat to life, health or safety or another permitted general situation or another permitted health situation exists.

Storage and security of your personal information

We store personal information in a variety of formats including on databases, in hard copy files and on personal devices, including laptop computers.

The security of your personal information is of paramount importance to us and we take all reasonable steps to protect the personal information we hold about you from misuse, loss, unauthorised access, modification or disclosure.

These steps include:

- Restricting access to information on our databases on a need to know basis with different levels of security being allocated to staff based on their roles and responsibilities and security profile.
- Ensuring all staff are aware that they are not to reveal or share personal passwords.
- Ensuring where sensitive information is stored in hard copy files that these files are stored in lockable filing cabinets in lockable rooms. Access to these records is restricted to staff on a need to know basis.
- Implementing physical security measures at our premises to prevent break-ins.
- Implementing ICT security systems, policies and procedures designed to protect personal information storage on our computer networks.
- Implementing human resources policies and procedures, such as email and internet usage, and confidentiality policies, designed to ensure that staff follow correct protocols when handling personal information.
- Undertaking due diligence with respect to third party service providers who may have access to personal information, including customer identification providers and cloud service providers, to ensure as far as practicable that they are compliant with the Australian Privacy Principles or a similar privacy regime.

Personal information we hold that is no longer needed, or required to be retained by any other laws, is destroyed in secure manner, deleted or de-identified as appropriate.

Our website may contain links to other websites. We do not share your personal information with those websites and we are not responsible for their privacy practices. Please check their privacy policies.

When we disclose your personal information

We only use personal information for the purposes for which it was given to us, or for purposes which are directly related to one or more of our functions or activities. We may disclose your personal information to government agencies, and other recipients from time to time, only if one or more of the following apply:

- you have consented;
- you would reasonably expect us to use or disclose your personal information in this way;
- we are authorised or required to do so by law;
- disclosure will lessen or prevent a serious threat to the life, health or safety of an individual or to public safety;
- where another permitted general situation applies or another permitted health situation exists;
- disclosure is reasonably necessary for a law enforcement related activity.

Disclosure of your personal information to overseas recipients

We may disclose personal information about an individual to overseas organisations that help us provide our services, in certain circumstances, such as when storing information with a “cloud service provider” which stores data outside of Australia. We will however take all reasonable steps not to disclose an individual’s personal information to overseas recipients unless:

- we have the individual’s consent (which may be implied);
- we have satisfied ourselves that the overseas recipient is compliant with the Australian Privacy Principles, or a similar privacy regime;
- we form the opinion that the disclosure will lessen or prevent a serious threat to the life, health or safety of an individual or to public safety; or
- we are taking appropriate action in relation to suspected unlawful activity or serious misconduct

How we ensure the quality of your personal information

We take all reasonable steps to ensure the personal information we hold, use and disclose is accurate, complete and up-to-date. These steps include ensuring that the personal information is accurate, complete and up-to-date at the time of collection and when using or disclosing the personal information.

On an ongoing basis we maintain and update personal information when we are advised by individuals or when we become aware through other means that their personal information has changed.

Please contact us if any of the details you have provided change. You should also contact us if you believe that the information we have about you is not accurate, complete or up-to-date.

How to gain access to your personal information we hold

You may request access to the personal information we hold about you, or request that we change the personal information, by contacting us.

If we do not agree to provide you with access or to amend your personal information as requested you will be notified accordingly. Where appropriate we will provide you with the reason/s for our decision. If the rejection relates to a request to change your personal information you may make a statement about the requested change and we will attach this to your record.

Privacy Complaints

If you wish to make a complaint about a breach by us of the Australian Privacy Principles, you may do so by providing your written complaint by email, letter, facsimile or by personal delivery to any one of our contact details as noted below. You may also make a complaint verbally.

We will respond to your complaint within a reasonable time (usually no longer than 30 days) and we make seek further information from you in order to provide a full and complete response.

Your complaint may also be taken to the Office of the Australian Information Commissioner.

How To Contact Us

You can contact us about this Privacy Policy or about your personal information by:

- Emailing info@healthreimagined.com.au
- Calling (07) 4044 8900
- Writing to our Privacy Officer at PO Box 1056, Bungalow, QLD 4870

If practical, you can contact us anonymously (i.e. without identifying yourself) or by using a pseudonym. However, if you choose not to identify yourself, we may not be able to give you the information or provide the assistance you might otherwise receive if it is not practical to do so.

Changes to our privacy and information handling practices

This Privacy Policy is subject to change at any time.