



QUEENSLAND COUNTRY HEALTH FUND LTD

PRIVACY POLICY

Queensland Country Health Fund Ltd (the Health Fund) recognises the importance of Members' privacy, and is committed to protecting personal information about Members that the Health Fund holds. This Privacy Policy describes how the Health Fund manages Members' personal information and safeguards Members' privacy.

1. NATIONAL PRIVACY PRINCIPLES

From 21 December 2001, most private sector organisations in Australia must by law comply with the National Privacy Principles ("NPPs") contained within the Privacy Act 1988. The NPPs strengthen protection of Member's privacy. Queensland Country Health Ltd (the Health Fund) will comply with the NPPs from that date.

2. COLLECTING PERSONAL INFORMATION

The Health Fund holds only those kinds of personal information that are necessary for the Health Fund to perform its functions. This in turn depends upon the type of product or service Members request. It may include:

- 2.1 Information Members give the Health Fund when applying for or requesting a product or service from the Health Fund. The information will include the Member's name, address, contact details, date of birth, previous or current private health insurance and may include financial institution details. If the Member fails to give the Health Fund the information asked for, the Health Fund may be unable to process the Members request for a product or service.
- 2.2 Health information about Members, such as pre-existing ailments and medical conditions. The Health Fund will only hold information obtained regarding health information if the Member has authorised the Health Fund to collect the information. This authorisation may be through the signing of an application form requesting health insurance, authorising the transfer of health insurance from another health fund or through the submission of a claim for processing.
- 2.3 Communications between Members and the Health Fund.
- 2.4 Transactional information about a product or service the Member has or has had with the Health Fund or has or has had paid by the Health Fund.

If personal information concerns particular topics it is regarded as sensitive information. Sensitive information can be information about racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record or health. Collection of health information by the Health Fund is necessary to provide health services to Members. This information is collected as required by law or in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality that bind the organisation. The Health Fund only collects, uses or discloses sensitive information about Members as is allowed by law.

The Health Fund may also collect some information about Members when they use the Health Fund's website <http://health.qccu.com.au> ("the website"):

- when Members visit the website, the Health Fund's server may attach a small data file, called a cookie, to the hard drive for the Health Fund's record keeping purposes. The Health Fund does not store any information inside cookies. Cookies are a feature of most websites. Most web browsers are set to accept cookies, but may be set to refuse them. If the Health Fund uses cookies it would be to provide aggregate and anonymous information on how people use the website and what they find interesting and useful on it. The Health Fund would not link this information back to any information Members have otherwise provided.
- as most websites do, the Health Fund tracks usage patterns on an anonymous and aggregate basis. A Member's identity cannot reasonably be ascertained from this information. Each time the website is visited, a web server records the visit, and

information that includes Member's internet provider's address, the date and time of the visit, the pages accessed and documents downloaded and any search items entered.

- if Members visit the website to complete an online form or to send an email to the Health Fund, the Health Fund will record the information given, including email addresses.

Thus, Members use of the facilities and information available on the website will determine the type and amount of personal information the Health Fund collects about Members.

3. USING AND DISCLOSING PERSONAL INFORMATION

- 3.1 The Health Fund respects Members' privacy. Any personal information which the Health Fund collects about Members will be used to:
- (a) provide Members with the products or services they have requested; or
 - (b) assess an application by Members for products or services the Health Fund may provide and if that application is approved, to provide them to Members; or
 - (c) assess health insurance benefits payable on Members' claims; or
 - (d) to pay Members' claims to their nominated financial institution.

In addition, the Health Fund may also use Member's personal information to provide them with information about other products and services offered or distributed by the Health Fund or any related company(ies). If Members do not want to receive any of this information they can contact the Health Fund. Often the law requires the Health Fund to provide Members with certain information about the product or service that they have received from the Health Fund. Members will continue to receive this type of information from the Health Fund even if they have decided not to receive information about the Health Fund's products and services generally. Where possible, the Health Fund stores any personal information about Members anonymously. The Health Fund does not use external identifiers to assist in the management of personal information.

- 3.2 The Health Fund stores Members' personal information with a strong emphasis on its security and the protection of Members' privacy. In considering the security of Members' personal information, the Health Fund has taken into account:

- (a) Physical security:
 - (i) All files containing personal information are stored securely on premises during and after business hours.
 - (ii) All files containing personal information are accessible only by staff requiring them for the completion of specific duties.
 - (iii) Drafts, spare copies and extra materials generated in the handling of files containing personal materials are destroyed by means of a secure destruction service.
 - (iv) Personal information that is no longer required is permanently de-identified or destroyed by means of a secure destruction service.
 - (v) Information about resigned Memberships is securely stored and is destroyed by means of a secure destruction service in accordance with legislative time frame requirements.
- (b) Computer and network security:
 - (i) Access to the computer network is by user identification and password only. Passwords are changed regularly. The system administrator can identify all users by their user identification.

- (ii) The system administrator regularly reviews computer logs for security breaches and reports any breaches to the relevant manager.
 - (iii) Computer files are regularly reviewed for continued relevance by a staff member of an appropriate security level and where necessary deletion and purging of files no longer required is undertaken on a system wide basis.
 - (iv) Files are regularly backed up and saved at a separate and secure site.
 - (v) Network security includes firewall and virus protection and network intrusion detection systems.
- (c) Communications security:
- (i) No personal information is provided at our offices, over the telephone or by facsimile until the identity of the applicant is verified.
- (d) Personnel security:
- (i) Hard file and computer copies of unsuccessful applications for employment are destroyed by means of a secure destruction service. Appropriate and lawful enquiries are made before an offer of employment is made to any person.
 - (ii) Access to Members' personal information is given to staff strictly on the basis of their need to have access to the material in order to fulfill their function within the Health Fund.
- 3.3 In order to provide Members with information about other products and services offered or distributed by the Health Fund or any related company(ies), the Health Fund may disclose Members' personal information to:
- any related company(ies)
 - organisations to whom the Health Fund contract out functions (e.g. information technology services and mailing houses)
- 3.4 The Health Fund contracts out some of its functions, as mentioned above, to external service providers. The Health Fund may disclose Members' personal information to them so that they can provide the services the Health Fund has contracted out to them. Where possible, all the Health Funds service providers are subject to the NPPs or, where practical, to arrangements imposing confidentiality requirements on them.

4. ACCESS TO PERSONAL INFORMATION

- 4.1 From 21 December 2001, in most cases, Members can gain access to personal information the Health Fund holds about them. The Health Fund will handle requests for access to Members' personal information in accordance with the NPPs. All requests for access to Members' personal information will be handled by the Privacy Access Officer, who can be contacted in writing at the postal address set out in item 5 below.
- 4.2 The Health Fund will deal with all requests for access to personal information as quickly as possible. In any event, the Health Fund will make an initial response to Members' requests within 30 days. Requests for large amounts of information, or for information not currently in use, may require some time before a full response can be given.

- 4.3 In some circumstances under the NPPs the Health Fund may refuse to give Members access to personal information held about them. These are circumstances where giving Members access would:
- (a) pose a serious and imminent threat to the life or health of any individual;
 - (b) have an unreasonable effect upon the privacy of other individuals;
 - (c) give access to material which would not be accessible by the process of discovery in existing or anticipated legal proceedings between the Member and the Health Fund;
 - (d) reveal the Health Fund's intentions in relation to negotiations with Members in such a way as to prejudice those negotiations;
 - (e) be unlawful;
 - (f) be likely to prejudice an investigation of possible unlawful activity, or
 - (g) be likely to prejudice:
 - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, or certain other breaches of law;
 - (ii) the enforcement of laws relating to the confiscation of the proceeds of crime;
 - (iii) the protection of the public revenue;
 - (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct, or
 - (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders; by or on behalf of an enforcement body.

The Health Fund may also refuse access if:

- the request for access is considered frivolous or vexatious;
- it is required or authorised by or under law to do so; or
- an enforcement body performing a lawful security function asks the Health Fund not to do so, on the basis that to do so would be likely to cause damage to the security of Australia.

If the Health Fund refuses to give Members access to the personal information they request, the Health Fund will under the NPPs provide Members with reasons for the refusal.

- 4.4 The Health Fund wishes to ensure that Members' personal information is accurate, complete and up to date. Generally, if Members request the Health Fund to do so, the Health Fund will amend any personal information about Members that is inaccurate, incomplete or out of date. If the Health Fund disagrees with a Member about any of these matters, and if the Member requests the Health Fund to do so, the Health Fund will take reasonable steps to associate a statement to the effect that the Member claims the information to be inaccurate, incomplete or out of date with their personal information.
- 4.5 There will be no charge for lodging a request for access to personal information. However, the Health Fund may charge Members for providing access. Any charges will not be excessive.
- 4.6 Members often have one or more Dependants covered by private health insurance under a Membership. Personal information concerning a Member or any Dependants covered by a Membership is confidential to the individual and is not accessible by any other person within that Membership. The only exception to this is where the Health Fund is able to reasonably determine that a person is incapable of determining their privacy rights.

5. HEALTH FUND CONTACT INFORMATION

Members can get more information about the way the Health Fund manages personal information about them by contacting the Health Fund at the postal address set out below. If Members are concerned that the Health Fund may have breached their privacy and wish to make a complaint, they can contact the Health Fund at the postal address set out below.

Contact details

- If Members wish to:
 - request a change to personal information held;
 - access their personal information;
 - receive further information about the way the Health Fund manages personal information; or
 - complain about a breach of privacy

they can write to Privacy Access Officer PO Box 42, Aitkenvale, Qld 4814.

- If Members are not satisfied with the Health Fund's response to their complaint they can contact the Federal Privacy Commissioner:

Director of Complaints
Office of Federal Privacy Commissioner
GPO Box 5218
Sydney NSW 1042

6. CHANGES TO THE HEALTH FUND'S PRIVACY POLICY

- 6.1 It is a policy of the Health Fund that communication of this Privacy Policy be made to the primary Member under a Membership and that it is the responsibility of that Member to ensure, where possible, that all Dependents under the Membership read and understand this Policy.
- 6.2 From time to time it may be necessary for the Health Fund to review and revise the privacy policy. The Health Fund reserves the right to change the privacy policy at any time. If the Health Fund does change this privacy policy the Health Fund will post amended versions in its offices and post an updated version on the website.

This Privacy Policy is effective from December 21, 2001