



## Policy Statement

RHealth is committed to dealing with personal information acquired during its operations and activities in accordance with relevant legislation.

RHealth personnel are aware of their privacy obligations as they relate to their roles and the organisation's activities. RHealth contractors are required to comply with privacy obligations as it relates to their contractual engagement.

This Policy will be enacted by aligning RHealth's processes and practices with the Australian Privacy Principles (APPs) and other relevant legislation, as appropriate. The Privacy Policy Appendix outlines the applicability of the APPs to RHealth's operations and includes an outline of what information RHealth deals with and how it is used and managed.

Where there is the potential for serious harm as a consequence of a breach of privacy obligations, RHealth's Data Breach Policy should be read in conjunction with this Privacy Policy. RHealth's Information Security Management documentation also enables compliance with privacy requirements and expectations.

## Rationale

RHealth is a registered Australian public company limited by guarantee as well as a large charity organisation. RHealth's purpose is to support the health and wellbeing of communities. To successfully and safely deliver on that purpose, RHealth needs to access personal information related to such activities as the engagement of required personnel and contractors, and the delivery of health-related services to consumers.

The information that RHealth accesses may include sensitive health information that RHealth acknowledges requires particular handling and protective processes.

As required by applicable legislation, this policy establishes RHealth's Privacy Policy approach as a means of outlining and identifying how RHealth manages the personal information it requires to operate effectively.

## Scope

All RHealth Board members, employees, students and volunteers (RHealth personnel) are to comply with this policy.

RHealth will require its subcontractors to operate in accordance with privacy legislation as it pertains to their contract.

The Policy Appendix outlines the full scope of parties that this policy relates to (at 1.3) and they are collectively referred to as key interested parties for the purposes of this policy.

This policy should be considered in conjunction with RHealth's Data Breach Policy and information Security Management documentation.

## Responsibilities

All RHealth personnel are responsible for dealing with and managing personal information they have access to in accordance with relevant legislation. The main legislation that guide's RHealth's privacy practices in relation to personal information, is the Commonwealth Privacy Act 1988 and its associated Australian Privacy Principles – see this Policy's Appendix. Other legislation that relates to privacy or deals with specific

privacy requirements or exceptions, are also to be adhered to as relevant to RHealth’s activities – see related legislation below for examples.

In accordance with the RHealth Risk Management Policy, RHealth Management and Leads should identify and control privacy compliance risk.

RHealth will provide appropriate education, training and awareness opportunities and resources to all RHealth employees, students and volunteers (RHealth personnel) to support their responsibilities under this policy.

If privacy risk controls prove to be inadequate, RHealth personnel shall report breaches of this policy and its associated procedures to their line manager via incident reporting processes, in alignment with the RHealth Incident Management Policy.

RHealth requires contractors to comply with all privacy related laws and regulations as they relate to the services RHealth engages them to provide. RHealth may undertake checks to ensure contractor compliance with privacy requirements.

**Related legislation, policies and resources**

Relevant legislation and standards include but are not limited to:

- Privacy Act 1988 (Cth)
- Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)
- Cyber Security Act 2024 (Cth)
- RHealth Data Breach Policy
- RHealth Incident Management Policy
- RHealth Information Security Management documentation
- Healthcare Identifiers Act 2010 (Cth)
- Information Privacy Act 2009 (Qld)
- Fair Work Act 2009 (Cth)

**Stewardship, version control & review**

<b>Executive Sponsor</b>	General Manager	
<b>Author</b>	Quality & Assurance Lead	
<b>Approval Authority</b>	RHealth Board	
<b>Readership</b>	All RHealth staff, students, volunteers and interested stakeholders	
<b>Version</b>	<b>Date Approved</b>	<b>Due for Review</b>
1	12 Oct 2022	Oct 2025
1.1	14 May 2025	2028 – or earlier if need identified



# Privacy Policy

**Classification:** Internal

**Readership:** ISMS Implementation Team



# Contents

1	Introduction .....	3
1.1	Purpose .....	3
1.2	Commitment .....	3
1.3	Scope of Application .....	4
2	Privacy Terms Used.....	4
3	Privacy of Personal Information .....	6
3.1	Open and Transparent Management of Personal Information .....	6
3.2	Anonymity and Pseudonymity .....	6
3.3	Collection of Solicited Personal Information .....	6
3.4	How We Deal with Personal Information We Didn't Ask For .....	8
3.5	To Whom Do We Disclose Personal Information.....	9
3.6	Use and Disclosure for Direct Marketing .....	10
3.7	Transfer of Information outside Australia/Cross-border Disclosure of Personal Information .....	11
3.8	Adoption, Use or Disclosure of Government Related Identifiers .....	11
3.9	Quality and Integrity of Personal Information .....	11
3.10	Security of Personal Information .....	11
3.11	Access to Personal Information .....	12
3.12	Correction of Personal Information .....	13
3.13	Privacy Incident Management .....	14
4	Privacy Complaints and How RHealth Would Deal with A Complaint.....	14
5	Policy Review and Amendment .....	14



## 1 INTRODUCTION

### 1.1 PURPOSE

The purpose of RHealth's Privacy Policy is to outline RHealth's commitment to protecting the privacy of individuals and how RHealth complies with its confidentiality and privacy obligations. As RHealth's activities include the provision of health care and associated health and community support services, RHealth is required, by law, to comply with relevant Commonwealth and State legislation relating to the handling and management of personal information. While there are recognised exclusions to the applicability of privacy legislation, like employee personal information, RHealth's privacy obligations extend to personal information it collects and maintains in relation to RHealth personnel (who include Board members, employees, students and volunteers), and contractors, as far as practicable.

This Appendix of the Privacy Policy explains how RHealth handles information and complies with the requirements of the Commonwealth Privacy Act 1988 (Cth) ("Privacy Act"), including the 13 Australian Privacy Principles (APPs) outlined in that Act. The APPs regulate how RHealth may collect, use, disclose, and store personal information and how individuals may access and correct personal information which RHealth holds about them. RHealth also recognises the possible applicability of the Information Privacy Act 2009 (Qld) through Queensland Government contracts and has assessed the requirements of the state privacy legislation as being encompassed by national requirements.

RHealth acknowledges that privacy is integral to professional practice associated with the provision of health care and other health and community support services, and as such, the 13 Australian Privacy Principles are adhered to in the collection, security, access, correction, use and disposal of personnel, consumer or contractor personal and/or sensitive information including:

1. Open and transparent management of personal information
2. Anonymity and pseudonymity
3. Collection of solicited personal information
4. Dealing with unsolicited personal information
5. Notification of the collection of personal information
6. Use or disclosure of personal information
7. Direct marketing
8. Cross-border disclosure of personal information
9. Adoption, use or disclosure of government related identifiers
10. Quality of personal information
11. Security of personal information
12. Access to personal information
13. Correction of personal information.

Further information on how RHealth ensures compliance with privacy obligations across its varied services and programs can be found in the RHealth Programs & Operations Manual and service/program specific manuals.

### 1.2 COMMITMENT

RHealth takes privacy seriously and is committed to complying with Australian privacy laws through:

- a. honouring its duty of care in relation to safeguarding personal information and related



communications and disclosures,

- b. by ensuring systems and procedures are in place, and practices are implemented, that will ensure compliance with the Privacy Act 1988 (Cth), including the 13 Australian Privacy Principles (APP's), and the Information Privacy Act 2009 (Qld) as applicable.

Having the confidence of key interested parties (RHealth personnel, consumers, contractors) is an organisational and professional privilege that will be respected at all times. This includes the right of key interested parties to provide informed consent to the collection of information as part of their relationship with RHealth.

### **1.3 SCOPE OF APPLICATION**

This Policy **relates** to all RHealth key interested parties including:

- a. RHealth's Board of Directors
- b. RHealth employees including those that operate within the following scopes of employment:
  - employed clinicians delivering services under funded programs
  - non-clinicians providing health and community support services under funded programs
  - information technology (IT) and data staff who support and maintain digital information systems accessed and used by RHealth employees and other services and organisations
  - staff who access and/or manage RHealth employee personal information
- c. students on placement within RHealth's programs or services
- d. RHealth sub-contracted health professionals and service providers
- e. RHealth volunteers
- f. organisations and sub-contractors RHealth engage to support the development and maintenance of RHealth's information storage systems
- g. external and internal users of RHealth's information storage systems
- h. consumers of RHealth delivered or sub-contracted services
- i. organisations who fund and/or contract RHealth to provide and maintain digital information sharing platforms
- j. organisations and agencies that in accordance with contractual obligations, take receipt of de-identified information from RHealth's digital information systems

For the purpose of this Privacy Policy, the term '**key interested parties**' will be used to collectively refer to the above individuals and organisations.

## **2 PRIVACY TERMS USED**

**Personal Information**

*Personal Information* (as it is defined in the Privacy Act 1988 (Cth) means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- a. whether the information, or opinion, is true or not; and
- b. whether the information, or opinion, is recorded in a material form or not.

**Sensitive Information**

*Sensitive Information* means information or an opinion about an individual such as race or ethnic origin, political opinions/associations or religious or philosophical beliefs, criminal record, sexual preferences, professional or health information and



records, biometric information used for biometric verification or identification, criminal history checks, working with children checks, income and bank details, and grievances, etc.

It includes personal and sensitive information that is maintained digitally, in case notes, employee files, on video, audio cassette, photographed, written/printed or verbal information given by, or about, a customer, a staff member, a volunteer or contractor to an RHealth staff member. It also includes professional opinion/s if the individual can be identified from that opinion/information.

Information which is '*sensitive information*' attracts a higher privacy standard under the Privacy Act 1988 (Cth) and is subject to additional mechanisms for an individual's protection.

**Health Information** *Health Information* as defined in the *Privacy Act 1988* (Cth) is a particular subset of '*sensitive information*' and means information, or an opinion, about:

- a. all identifying "personal information" collected to provide a health service;
- b. the health, including illness, disability or injury, (at any time), of an individual; or
- c. an individual's expressed wishes about the provision, to them, of health services; or
- d. a health service provided or to be provided to an individual that is also personal information.

**Consent** *Consent* means '*expressed consent or implied consent*'. The four key elements of consent are:

- the client is adequately informed before giving their consent;
- the client gives consent voluntarily;
- the consent is current and specific; and
- the client has the capacity to understand and communicate their consent.

**Note:** Willingly provided information is usually sufficient to imply consent to collection of information; however, RHealth may seek written client consent before collecting personal health information in some circumstances.

**Expressed Consent** *Expressed consent* is given explicitly, either orally or in writing.

**Implied Consent** *Implied consent* arises where consent may reasonably be inferred in the circumstances from the conduct of the key interested parties and RHealth.

**Solicited and Unsolicited Personal Information** All personal information received by RHealth is either solicited or unsolicited personal information. Personal information received by RHealth that does not fall within the definition of *solicited* is *unsolicited* personal information.



### **3 PRIVACY OF PERSONAL INFORMATION**

#### **3.1 OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION**

RHealth makes this Privacy Policy and related material available to RHealth key interested parties to inform about the organisation's Policy and practices for the management of personal information. The Privacy Policy will primarily be available through RHealth's website but can be provided via other communication mediums upon request.

Information collected about;

- service consumers will be for the prime purposes of delivering contracted services, which may include the direct or indirect provision or support of health care and community services,
- RHealth personnel, contracted service providers and other service stakeholders, will be for the prime purpose of recording information related directly to their employment, engagement and work, for or with RHealth.

As appropriate, individuals will be informed about the kind of personal information that will be collected, the reason it is being collected, how the information will be collected, stored and used, and how it can be accessed and updated.

#### **3.2 ANONYMITY AND PSEUDONYMITY**

Parties that interact with RHealth have the right to be dealt with anonymously or by using a pseudonym, provided that this is lawful and practicable. It may be impracticable for RHealth to deal with parties who have not identified themselves. For example, in the health service provision context, anonymity of pseudonymity is not likely to be practical or possible:

- a. due to contractual requirements of funded programs;
- b. for Medicare and insurance rebate purposes where applicable and relevant; and
- c. where a client complains about any aspect of health care/service delivery, which for the purposes of further investigation RHealth would need to know the details of the client involved in the complaint and other details which would enable RHealth to identify the health care and other service providers involved.

Neither can RHealth deal with its employees or contractors in an anonymous manner.

RHealth will inform individuals about consequences relating to anonymity of pseudonymity where relevant and appropriate.

#### **3.3 COLLECTION OF SOLICITED PERSONAL INFORMATION**

RHealth is a provider or facilitator of health-related services and associated health and community support services and therefore, it is sometimes necessary for RHealth employees and sub-contractors to collect information from individuals that is required for the provision of services. Individual personal and health information can help identify which course of service delivery is likely to be safe and effective and may identify health concerns which can receive early intervention. The collection of personal health information may also reduce the likelihood of repeated unhelpful service provision.

RHealth employees and sub-contractors will only ask for information where it is believed to be necessary for optimal service provision. Health information will only be collected where specified requirements are met, including:

- a. with the relevant individual's consent; or
- b. when collection is required, authorised or permitted by law or law enforcement purposes; or



- c. the information is received, through an appropriate disclosure by another organisation such as another health service provider with the individual's consent; or
- d. the collection is necessary to prevent or lessen a serious threat to life, health or safety of an individual or the public.

RHealth will ensure that individuals providing personal information are informed about and understand the purpose of collecting the information, to whom or under what circumstances their personal information may be disclosed to another party, and how they can access the information held about them by RHealth. If an individual is physically or legally incapable of providing consent, a responsible person (as described in the legislation) may do so.

### **3.3.1 What Happens if You Do Not Provide Health Information**

RHealth will ensure that individuals providing personal information understand the consequences, if any, of providing incomplete or inaccurate information. A consequence may be that RHealth or its contractor are unable to provide the individual with an optimal level of service, support or engagement.

### **3.3.2 Types of Personal Information Collected and Held**

The types of information collected by RHealth employees or contractors, may include an individual's:

- a. name, date of birth, address, email address, telephone number, ethnicity, demographics, next of kin, emergency contact details;
- b. employment information;
- c. financial information;
- d. other transactional information;
- e. Medicare, DVA and/or health fund details (as applicable);
- f. reason for attendance/symptoms;
- g. medical history;
- h. private health insurance information;
- i. examination and test results;
- j. diagnosis;
- k. treatment and care information; and
- l. admission and registration information.

RHealth or its contractors may also collect any other information necessary, or reasonably required, to provide the specific products and services other key interested parties require.

RHealth also may collect personal information from individuals when they meet with RHealth employees, communicate by letter, telephone, email or fax, provide a business card, or submit information through RHealth's website. RHealth may ask other people to analyse traffic on the RHealth website and may use cookies to do so.

To support inclusive practices and high-quality service provision to a diverse range of individuals or when contractually required by RHealth funders, RHealth may seek to collect sensitive personal information such as sexual preferences or practices, race and culture.

Other information collected and held by RHealth includes job applications, personnel files, contractor and referrer information.



### 3.3.3 Why We Collect Personal Information

RHealth and associated key interested parties collect personal information in order to:

- a. provide products and services to key interested parties;
- b. communicate with key interested parties;
- c. improve RHealth products and services;
- d. market RHealth products and services;
- e. send invitations to RHealth events;
- f. manage RHealth employees and contractors;
- g. fulfil legal and contractual obligations;
- h. exercise RHealth's legal rights and to issue or defend legal proceedings; and
- i. generally carry on RHealth business.

RHealth and relevant key interested parties require individual consent to collect and use personal information provided in the following ways:

- a. disclosure to others involved in the individual's healthcare including referring and/or treating doctors, specialists and other health professionals external to RHealth, which may occur through referral and referral follow-up;
- b. billing purposes, including compliance with Medicare and Health Insurance Commission requirements;
- c. for reminder letters which may be sent regarding ongoing health care and management;
- d. administrative purposes, in running RHealth as an organisation;
- e. to comply with any legislative or regulatory requirements; and
- f. for research, quality auditing and contractual reporting activities, as part of the quality review and continual improvement process, for accreditation purposes and to improve individual and community health care and organisational management. All information collected and reported for this purpose, will be de-identified, so that personal details will be protected.

### 3.3.4 How We Obtain your Information

RHealth collects information which is:

- a. provided directly by an individual;
- b. provided on an individual's behalf, with the individual's consent;
- c. received from a health service provider who refers an individual to an RHealth funded program or uses an RHealth owned online IT referral platform.

## 3.4 HOW WE DEAL WITH PERSONAL INFORMATION WE DIDN'T ASK FOR

Unsolicited personal information is personal information received by RHealth where RHealth has taken no active steps to collect the information. APP 4, Dealing with unsolicited personal information, outlines the steps RHealth must and will take if it receives unsolicited personal information.

When RHealth personnel or contractors receive unsolicited personal information, there will be an initial determination as to whether there would have been permission to collect the information under APP 3, 'Collection of Solicited Personal Information'. Such determination will be undertaken by an appropriate RHealth related individual, and they will consider whether the information is reasonably necessary for RHealth functions and if RHealth is permitted to hold the information in the same way as other information



the individual may have directly provided to RHealth.

- If so, APPs 5 through to 13 will apply to that information.
- If not, and no other legal reason exists for retaining the information, the information will be destroyed as soon as is practicable to do so.

In some instances, RHealth may have difficulty deciding whether personal information it receives falls within the terms of RHealth's request and is therefore solicited or unsolicited. Where it is unclear whether the information is solicited or unsolicited personal information, RHealth will err on the side of caution and treat the personal information as unsolicited personal information, and the information will be destroyed or de-identified in accordance with the APPs.

### **3.5 TO WHOM DO WE DISCLOSE PERSONAL INFORMATION**

As a provider and facilitator of health services or health-related support services, primarily in accordance with contractual requirements, RHealth may disclose personal information in a number of different ways, including deidentified, for different reasons.

RHealth employees and contractors will inform individuals of the reasons and circumstances of the probable disclosure of identified personal information, to provide the individual the right to decline consenting to such a disclosure. Individuals are to be informed of consequences, if any, of declining disclosure. If an individual is physically or legally incapable of providing or declining consent for disclosure, a responsible person (as described under the Act) may provide direction on their behalf.

RHealth may disclose collected personal information to RHealth contractors. For example, contractors may be engaged to provide products or services directly to RHealth or on behalf of RHealth. In addition, contractors may maintain and develop RHealth's customer records, IT systems and website. In such circumstances, RHealth will ensure contractors comply with privacy obligations.

RHealth's auditors, insurers and legal and other professional advisors may also access RHealth records, but only to protect RHealth interests and to ensure that RHealth complies with its obligations.

#### **3.5.1 When Personal Information Can Be Disclosed, With Your Consent**

The disclosure of **identified** personal information will always only be to facilitate optimal health service support or organisational insurance or legal requirements and will be with the individuals consent for the following purposes:

- a. to assist an individual's healthcare treating team (doctors, nursing staff and other Health Professionals) in providing health care to the individual;
- b. to provide necessary follow up treatment and ongoing care;
- c. to provide an individual with standard reminders, for example appointments and follow-up care; (these may be made by text message, email, letter or phone to the number or address which have been provided)
- d. to process private health fund, Medicare and/or DVA claims;
- e. for internal administrative requirements, including billing.

Information that has undergone an appropriate and robust **de-identification** process is not personal information and is therefore not subject to the Privacy Act. Whether information is personal or de-identified will depend on the context. Under contract or in accordance with the following circumstances, RHealth may be required to disclose **deidentified** information:

- a. organisational certification and accreditation activities;



- b. as part of the process of research, measuring outcomes, and continual quality improvement;
- c. contractual funding reporting;
- d. statistical reporting into national databases to support the review of healthcare funding policies.

### **3.5.2 When Information can be Disclosed Without your Consent**

RHealth will only disclose personal information without consent where such disclosure is required by law, or for law enforcement, or in the interests of the key interested parties' or the public's health and safety. For example,

- a. the disclosure is directly related to the primary purpose for collection;
- b. in an emergency situation, where release of information is necessary to aid medical treatment;
- c. when required by law to disclose the information (e.g. reporting of communicable diseases);
- d. when it is reasonably believed the individual is likely to harm themselves, or another person;
- e. when there is reason to suspect that a child may be at risk of sexual, physical or emotional abuse, or neglect; or
- f. when a key interested party believes the individual has committed a criminal act;
- g. when medical records are subpoenaed by a court;
- h. where failure to disclose information would place the individual or another person at serious and imminent risk (eg, emergency);
- i. where prior permission has been obtained to provide a written report to another professional or agency (eg, a GP or a lawyer) or discuss the material with another person (eg, a person authorised by you);
- j. to exchange information relating to an individual's program participation, and associated health and safety considerations with the people, organisations and agencies that an individual nominates;
- k. to address liability indemnity arrangements with insurers, medical defence organisations and lawyers;
- l. for the defence of anticipated or existing legal proceedings;
- m. for a directly-related secondary purpose that would have been within the reasonable expectations of the individual;
- n. if disclosure is otherwise required or authorised by law;

RHealth will keep records of any such disclosure.

## **3.6 USE AND DISCLOSURE FOR DIRECT MARKETING**

RHealth will only use or disclose personal information for direct marketing purposes where the individual has either consented to their personal information being used for direct marketing or has a reasonable expectation that their personal information will be used for this purpose. Individuals will be provided with opt-out mechanisms in these circumstances.

RHealth will seek key interested parties' permission for the use of personal or private information to undertake research and/or evaluation activities.

### **3.6.1 RHealth Website**

This Privacy Policy applies to any information RHealth collects via the RHealth website including information provided through enquiries. As per above, to ensure optimal website management, RHealth's website uses cookies for tracking website access and use.



### **3.7 TRANSFER OF INFORMATION OUTSIDE AUSTRALIA/CROSS-BORDER DISCLOSURE OF PERSONAL INFORMATION**

RHealth will take steps to protect key interested parties' privacy if information is to be sent interstate or outside Australia and will only transfer personal information overseas when:

- a. written consent is provided; or
- b. the transfer is necessary for the fulfilment of a contract between the individual and RHealth; or
- c. the transfer is for the individual's benefit, but it is impractical to obtain consent; or
- d. it is believed that the information will be protected by a privacy scheme or legal provisions comparable to those in Australia.

### **3.8 ADOPTION, USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS**

As required by Australian Privacy Principles (APP 9), RHealth will not use or disclose a government-related identifier unless an exception applies (eg, Medicare or Veterans Affairs numbers or other identifiers assigned by a Commonwealth or State Government agency) to identify personal information. For a definition of the term's 'identifier' and 'government-related identifier' please refer to Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth).

### **3.9 QUALITY AND INTEGRITY OF PERSONAL INFORMATION**

RHealth will take reasonable steps to ensure the personal information it collects, uses and discloses is relevant, accurate, up-to-date and complete, having regard to the purposes of such. To that end, RHealth encourages relevant key interested parties to contact RHealth to update or correct any personal information RHealth holds about them.

Key interested parties can request to correct or amend:

- a. information of a minor nature such as their personal contact details through discussion with RHealth; and
- b. more significant key interested parties' information such as file notes on the grounds that it is inaccurate, incomplete, out-of-date or misleading.

Approval for changes can only be granted by the RHealth management. A record will be kept of approved changes and what was changed. Requests to change documents, or records must have copies of all related correspondence kept in a confidential and secure file.

### **3.10 SECURITY OF PERSONAL INFORMATION**

RHealth will:

- a. take reasonable steps to protect the personal information it holds from interference, in addition to misuse and loss, and unauthorised access, modification and disclosure, including but not limited to
  - office and building security systems ensuring access-controlled premises and work areas
  - the required use of system password access to IT systems and servers
  - adequate computer system virus protections and fire wall
  - electronic back-up of records
  - directing RHealth personnel to undertake "clean desk" practices as appropriate – screens are privately viewed, computers are logged off and hard copy notes are locked away when personnel are not at the desk
- b. endeavour to take all reasonable steps to keep information accurate and up to date and not retaining



information once there is no longer a legal or business need to do so

RHealth requires all key interested parties to whom personal information is disclosed or whom may have access to personal information RHealth collects, to protect such personal information from misuse and loss and from unauthorised access, modification or disclosure.

### **3.10.1 What is Not Regarded as a Breach of Privacy and Confidentiality**

The following activities are not considered to be a breach of confidentiality or privacy as they are necessary for the proper discharge of professional services by RHealth:

- a. discussion of specific details during supervision, training, or consultation on a staff or RHealth service-related matter
- b. providing RHealth staff access to key interested parties' documents in order to analyse or maintain records and report to RHealth funding bodies, and key interested parties' statistics to RHealth Management, and during management system internal and external audits
- c. reporting of serious matters as required by law
- d. responding to a subpoena or court order to supply information, however it is noted that strict procedures are to be followed if a subpoena is served on any RHealth staff member or RHealth to produce documents and/or appear in court
- e. the sharing of employee information with external agencies for employment-related matters, for example, workers compensation claims, industrial relations matters, employment checks

### **3.10.2 How RHealth Holds your Personal Information**

RHealth takes all necessary and reasonable steps to ensure retained personal information is accurate, complete, up-to-date and secure. RHealth may store health information in both hard copy and digitally. The storage, use and where necessary, transfer of personal health information will be undertaken in a secure manner that protects key interested parties' privacy.

Hard copy information is kept under lock and key. Information stored on computer is password protected.

Information is collected from first contact through to exit from service or engagement and thereafter for the minimum records retention period for disposal, as specified by the relevant funding contract (where applicable), legislation or by the Queensland Government Archives policy and practices. After that time, if the record is no longer necessary, it will be disposed of securely as required by law.

## **3.11 ACCESS TO PERSONAL INFORMATION**

An individual may request access to their personal information held by RHealth. Requests for access should be made in writing and can be emailed to [admin@rhealth.com.au](mailto:admin@rhealth.com.au) or posted to the address listed below. RHealth deals with all requests for access to personal information as required by law.

RHealth needs to be satisfied that a request for personal information is made by the identified individual or by another person who is authorised to make a request on their behalf. An identity document will need to be sighted to verify the individual's identity or, if an individual authorises another person to access records on their behalf, then a letter of authority and confirmation of identity will be required prior to release of personal information.

A fee may be payable where RHealth incurs costs in providing access (including retrieval and the supply) to an individual's information. If applicable, the individual will be advised of the fee upon receipt of a request and access will be provided following receipt of payment.



RHealth will endeavour to process any request for access within 30 days of receiving the request. Some requests for access may take longer than 30 days to process depending upon the nature of the personal information being sought.

RHealth acknowledges the right of children to privacy of their health information. Based on the professional judgement of the relevant treating health professional or service provider, and consistent with the law, it might at times be necessary to restrict access to personal health information by parents or guardians.

### **3.11.1 Denying Access to Personal Information**

RHealth will provide access to information upon request by an individual, except in situations including but not limited to:

- where release is unauthorised by the owner of that information
- in situations where granting such access would infringe another person's privacy or a key interested parties' request for anonymity
- information where the information relates to existing or anticipated legal proceedings
- where denying access is required or authorised by law
- where the request for access is regarded as frivolous or vexatious
- generally, where there is no legal requirement to do so

If RHealth denies a request for access to personal information RHealth will provide the reasons for not doing so.

### **3.12 CORRECTION OF PERSONAL INFORMATION**

RHealth will take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading, if either:

- a. RHealth is satisfied that it needs to be corrected, or
- b. an individual requests that their personal information be corrected.

If an individual believes that information RHealth holds about them, or the organisation or other individual they are authorised to represent, is either incorrect or out of date, or if they have concerns about how RHealth handles their information, they can contact RHealth and RHealth will try to resolve those concerns. Key interested party personal information amendment requests should be made in writing and can be emailed to [admin@rhealth.com.au](mailto:admin@rhealth.com.au) or posted to the address listed below.

If RHealth does not agree to change personal information in accordance with a request, RHealth will provide the individual with written reasons for the refusal and notify them of available complaint mechanisms. RHealth will keep the request with the party's relevant records.

If a change is made, RHealth will endeavour to notify other relevant key interested parties that have been appropriately provided with the personal information of any correction, if that notification is requested by the individual.

RHealth will respond to a correction request or a request to associate a statement by the individual within a reasonable period after the request is made and will not charge the individual for making the request, for correcting the personal information, or for associating the statement with the personal information.



### 3.12.1 Updating Your Personal Information (APP 13)

If at any time, there is a belief that any personal information stored by RHealth is not accurate or is out of date, RHealth can be contacted on (07) 4638 1377 or email [admin@rhealth.com.au](mailto:admin@rhealth.com.au).

## 3.13 PRIVACY INCIDENT MANAGEMENT

Any suspected or perceived breaches of privacy will be investigated and reported in accordance with RHealth Incident Management Policy.

## 4 PRIVACY COMPLAINTS AND HOW RHEALTH WOULD DEAL WITH A COMPLAINT

RHealth is committed to improving services and welcomes any comments or complaints that key interested parties may wish to offer in relation to the services RHealth facilitates directly or through contract. Such feedback helps identify what RHealth does well or needs to improve. RHealth recognises that, handled well, a complaint provides an opportunity to strengthen relationships with key interested parties. It provides the opportunity to understand circumstances and to explore ways to improve services in the future. RHealth will respond to concerns quickly and in accordance with the RHealth Complaints Management Procedure (a copy of which can be provided upon request) and keep parties informed of actions and progress.

Complaints or queries with respect to this Privacy Policy may be lodged electronically via the RHealth website, or in writing by email or by completing an RHealth Feedback Form. Alternatively, you may contact:

RHealth Privacy Officer

PO Box 774 Toowoomba Qld 4350

Telephone: (07) 4638 1377

Email: [admin@rhealth.com.au](mailto:admin@rhealth.com.au)

Under the Privacy Act 1988 (Privacy Act) a complaint can be made to the Office of Australian Information Commissioner (OAIC) about the handling of personal information.

For further details, see <https://www.oaic.gov.au/individuals/what-can-i-complain-about>

## 5 POLICY REVIEW AND AMENDMENT

RHealth reserves the right to make changes or update this Privacy Policy from time to time to keep abreast of RHealth's changing operating environment or legislative changes. RHealth will post updated versions of the Privacy Policy on the RHealth website. Each time this Policy is changed it is given a new version, by date of update, which is visible in the footer of the document. When changes are made, RHealth will provide a notification via the RHealth website, for up to three months post update. Other notification methods may be considered when significant changes are made to the policy.

RHealth recommends that key interested parties regularly review RHealth's Privacy Policy to ensure they are aware of any changes.