

PRIVACY POLICY

Summary

The purpose of this document is to provide a framework for Ramahyuck District Aboriginal Corporation (The Corporation) in dealing with privacy considerations.

Policy

The Corporation and the Board of Directors is committed to protecting the privacy of personal information which the Corporation collects, holds and administers for the purposes of providing a variety of services and programs. Personal information is information which directly or indirectly identifies a person.

The Corporation is bound by the Australian Privacy Principles (APP) contained in the Commonwealth Privacy Act 1998, and is compliant with the Privacy Amendment (Enhancing Privacy Protection) Act 2012 and the Victorian Information Privacy Principles (IPP) contained in the Privacy and Data Protection Act 2014. In relation to health records, the Corporation is also bound by the Victorian Health Privacy Principles (HPP) contained in the Health Records Act 2001. Additionally, we are bound by the Children, Youth and Families Act 2005 (CYFA) and the Family Violence Protection Act 2008 (FVPA), which includes specific requirements and measures around the sharing of information – see exceptions.

We may, from time to time, review and update this Privacy Policy to take account of new laws and technology, changes to the Corporation's operations and practices and to make sure it remains appropriate to the changing legal environment.

Applicability

This policy is applicable to the Corporation's Directors, employees, contractors, volunteers, visitors and any other people who engage with the Corporation.

The Corporation's Board is responsible for developing, adopting and reviewing this policy.

The Corporation's Chief Executive Officer is responsible for the implementation of this policy, monitoring changes in Privacy legislation, and advising on the need to review or revise this policy as and when the need arises.

Privacy compliance is the responsibility of all employees, students or volunteers and other authorised users who handle personal, sensitive or health information.

Employees must not knowingly disclose nor direct another employee, volunteer or student to handle (including disclosing) information in a manner which will breach privacy obligations.

Exceptions under the CYFA, CWSA and FVPA

The Children, Youth and Families Act 2005, the Child Wellbeing and Safety Act 2005, and the Family Violence Protection Act 2008, govern the sharing of information held by the Corporation and privacy obligations. Ramahyuck District Aboriginal Corporation is a prescribed information sharing entity under both the *Child Information Sharing Scheme* and *Family Violence Information Sharing Scheme* and may disclose information provided in accordance with these schemes.

Generally, a client's information will not be shared without that client's informed consent. But if there is a serious threat to an individual's life, health, safety or welfare, information may be shared without a person's consent to lessen or prevent this serious threat.

Additionally, information may be shared without consent if this information is linked to a child victim survivor of family violence and it is necessary to assess or manage family violence risk to that child.

If a client's information is shared without consent, it will be done so in a manner that promotes the client's or other's safety and takes into account the client's views, where appropriate, safe and reasonable.

When appropriate, safe and reasonable the client will be notified about the information being shared.

Note: All staff that are required to observe this obligation will receive training and ongoing support to ensure as best as is practicable the appropriate application of legislated information sharing requirements.

Definitions

Definitions as per the relevant legislation will be applied to the processes within this policy. All legislation can be accessed in real time via <http://www.legislation.vic.gov.au/> and <https://www.legislation.gov.au/>

'Client' means, unless otherwise indicated, patient, consumer, customer, participant, or direct service user or person having membership with the Corporation.

'Information' means, unless otherwise indicated, sensitive, health or personal as appropriate to context.

'Must' means in the context of this document is a mandatory requirement. Breaching a mandatory requirement may lead to disciplinary actions as outlined in Disciplinary Process Policy and Procedure

The following procedures do not apply to:

- Personal information or data which is legitimately in the public domain;
- Personal information an individual has made public;
- Information that relates to corporate, government or business entities; or
- External websites that are linked to the Corporation website.

Related information

Legislation

- [Archives Act 1983 \(Commonwealth\)](#)
- [Child Wellbeing and Safety Act 2005 \(Vic\)](#)
- [Children, Youth and Families Act 2005](#)
- [Disability Act 2006 \(Vic\)](#)
- [Fair Work Act 2009 \(Commonwealth\)](#)
- [Family Violence Protection Act 2008 \(Vic\)](#)
- [Health Records Act \(VIC\) 2001](#)
- [Information Privacy Principles \(Vic\)](#)
- [National Disability Insurance Scheme Act 2019 C'wlth](#)
- [Occupational Health and Safety Act \(Vic\) 2004](#)
- [Privacy Act 1988 C'wlth](#)
- [Privacy and Data Protection Act 2014](#)
- [The Charter of Human Rights and Responsibilities Act 2006 \(Vic\)](#)

Regulations

- [The Child Wellbeing and Safety \(Information Sharing\) Regulations 2018](#)
- [The Family Violence Protection \(Information Sharing\) Regulations 2018](#)

Framework

- [The Family Violence Multi-Agency Risk Assessment and Management Framework](#)

- [The Family Violence Risk Assessment and Risk Management Framework](#)

Guidelines

- [Best Practice Guide Workplace Privacy](#)
- [The Family Violence Information Sharing Guidelines](#)

Corporation policies and procedures

- [Client Information Handbook Agreement](#)
- [Client Service Charter](#)
- [Complaint and Feedback Form](#)
- [Complaints Management Policy](#)
- Doc_1118_Client Handbook - includes client information privacy statement
- Doc_000 Privacy Information Collection Notice - Corporation (non-clients and non-employees)
- Doc_000 Privacy Information Collection Notice - E-recruitment
- Doc_1177_Privacy Information Collection Notice - HR
- Doc_000 Privacy Information Collection Notice - RDAC Members
- Doc_000 Privacy Information Collection Notice - Students
- Doc_000 Privacy Information Collection Notice - Volunteers
- [Informed Consent Policy](#)
- [Client File Management Policy](#)
- [Occupational Health and Safety Policy](#)
- [Personnel File Policy](#)
- [Privacy and Third Party Access to Health Information Policy medical Ops Manual](#)
- [Request for Personal Health Information Medical Ops Manual](#)
- [Scanning Documents and Digital Images Policy](#)
- [Security Screening Checks Policy](#)
- [Staff Confidentiality Agreement](#)
- [Staff Immunisation Policy](#)
- [Telephone Calls Policy](#)
- [Verbal or Written Reference Policy](#)
- [Your rights when you use health services in Victoria](#)

PROCEDURES

Collection of personal information

The type of *information* the Corporation collects and holds includes (but is not limited to) health and personal, including sensitive information. We will:

- Collect only *information* which the Corporation requires for its primary functions;
- Ensure that stakeholders are informed as to how we administer the *information* gathered;
- Use and disclose *information* only for our primary functions or a directly related and reasonably expected secondary purpose, or for another purpose with the person's informed consent; some exceptions exist.
- Take reasonable steps to inform persons of the purpose of collection and the use and disclosure of the *information*, through the use of 'Privacy Information Collection Notices';
- Store *information* securely, protecting it from unauthorised access; and
- Provide stakeholders with access to their own *information*, and the right to seek its correction.
- Take reasonable steps to ensure the *information* held is accurate, complete, up-to-date and relevant to the Corporations functions, activities, services and programs.

Information you provide:

The Corporation will generally collect personal, sensitive or health information held about an individual by way of: phone calls, forms, meetings, emails, appointments, voice mail messages, test results, medical histories, sick leave certificates, etc. Only *information* that is necessary to fulfill the functions and activities of the Corporation will be collected.

You do have the right to seek to deal with us anonymously or using a pseudonym, but in almost every circumstance it will not be practicable for us to deal with you or provide any services to you except for the most general responses to general enquiries, unless you identify yourself.

Information provided by other people:

Where practicable, we will collect personal or sensitive information directly from you. In some circumstances the Corporation may be provided with personal or sensitive information about an individual from a third party, for example Child Protection.

How will the Corporation use the information you provide?

We will use *information* we collect from you for the primary purpose of collection, and for such other secondary purposes that are related to the primary purpose of collection and reasonably expected, or to which you have consented. Such collection will be by lawful and fair means and will not be unreasonably intrusive.

The type of *information* collected will be determined by the nature of the service or support you request from us. To provide detailed information relating to the handling of personal information, we have adopted a number of 'Privacy Information Collection Notice' documents based on the type of service or support provided to you.

We may use video surveillance for security purposes and the footage will be used only by the Corporation and by the providers of our security services for security purposes. Surveillance videos are not used by the Corporation for other purposes and the footage is not publicly available. Surveillance cameras are not located in any bathrooms or change room facilities.

Data Breach Notification

The Corporation accepts its obligation to keep *information* safe and is open and transparent in how data is handled. In the event that personal data systems are breached, data is misused or lost, we will take all reasonable and practicable means to contact individuals whose *information* is involved. We will advise such individuals of the extent of the data breach (if known) and advise individuals of the most appropriate means of regaining control of their *information*, in an effort to limit the personal impact of the breach. If appropriate, Ramahyuck District Aboriginal Corporation will also report any breach of data to the Office of the Australian Information Commissioner (OAIC). We will also report breaches to the Office of the Victorian Information Commissioner (OVIC) as appropriate, based on our responsibilities as a contracted service provider to the state government under the PDP Act. Our data breach response plan includes a data breach procedure flowchart, explains how this will occur.

Opting out of receiving material produced by the Corporation:

If you are an employee or member or client and you do not wish to receive communications from us, you can opt out by utilising the unsubscribe options on the specific publication.

Alternatively, a written request can be sent to the Corporations **Privacy Officer** at privacyofficer@ramahyuck.org detailing the communications you no longer wish to receive.

Some Corporation communications are not optional and must continue to enable the Corporation to operate effectively.

In relation to employee records:

In many cases the State and or the Commonwealth privacy laws will not apply when it comes to employee records. As a result, the Corporation has chosen to observe the Fair Work Ombudsman's *Best Practice Guide (2014)* in relation to the treatment of an employee record. However, the Corporation must provide access and ensure compliance with the *Health Privacy Principles* under the Victorian *Health Records Act 2001*. See '*doc_000 HR - Privacy Information Collection Notice*'

Job applicants:

In relation to personal information of job applicants, staff members and contractors, the Corporation's primary purpose of collection is to assess and (if successful) to engage the applicant, staff member or contractor, as the case may be. See '*doc_000 Privacy Information Collection Notice - E-recruitment*'.

Where the Corporation receives unsolicited job applications these will usually be dealt with in accordance with the unsolicited personal information requirements of the *Privacy Act*.

Students and Volunteers:

The Corporation also obtains personal information about volunteers or students who assist the Corporation in its functions or conduct associated activities, such as to enable the Corporation and the volunteers and or students to work together. See '*doc_000 Privacy Information Collection Notice - Volunteers*' and '*doc_000 Privacy Information Collection Notice - Students*'

Staff members and contractors:

If you are an employee seeking access to your personnel file, you may lodge a request in writing to the Human Resource section: Attention to the '*Workforce Capability and Culture Manager*'. Should you wish to access other personal documents not held in your personnel file, e.g., a Medical file, you must lodge a request in accordance with the Corporation's appropriate policy and procedures to the **Privacy Officer**.

Who might the Corporation disclose personal information to?

The Corporation may disclose *information*, including sensitive information, held about an individual to:

- Government departments;
 - People providing services to the Corporation, and
 - Anyone you authorise the Corporation to disclose information to;
- Where the use or disclosure is required or authorised by or under law; see exceptions on page 2 of this document
- Other exceptions apply in the *APP*, *IPP* and the *HPP* refer to the particular legislation for further details.

In addition, personal (including sensitive and /or health information) may be used or disclosed if it is necessary to lessen or prevent:

- A serious threat to your life, health, safety or welfare: or
- A serious threat to public health, public safety or public welfare.
- Where the use or disclosure is required or authorised by or under law.

More detailed information is outlined in the applicable '*Privacy Information Collection Notice*' which are provided at the time *information* is collected or as soon as practicable thereafter.

Sending information overseas:

The Corporation will not send personal information about an individual outside Australia without:

- obtaining the consent of the individual (in some cases this consent will be implied); or
- otherwise complying with the *IPP*, *APP* or *HPP* or other applicable privacy legislation.

Note: We do not use overseas providers of IT services including servers and cloud services.

How does the Corporation treat information?

Information will be used and disclosed only for the purpose for which it was provided or a directly related secondary purpose, unless you agree otherwise, or the use or disclosure of the *information* is required or authorised by or under law.

Management and security of information:

Our staff are required to respect the confidentiality of *information* and the privacy of individuals.

We take reasonable steps to ensure that personal, sensitive and health information we collect, maintain, use or disclose is:

- Accurate, complete and up to date;
- Protected from misuse, loss, unauthorised access, modification or disclosure; and
- Securely destroyed or permanently de-identified when no longer required in accordance with our management of files policy, doc_464. In some circumstances, however it will be kept for marketing purposes, as you will have consented to that in writing with us.
- Securely stored by way of locked cabinets and secured areas for paper records and password protected access rights to computerised records.

When you use our website, having your cookies enabled will allow us to maintain the continuity of your browsing session and remember your details when you return. We may also use web beacons, Flash local stored objects and JavaScript. If you adjust your browser settings to block, reject or delete these functions, the webpage may not function in an optimal manner. We may also collect information about your IP address, although this may not identify you.

Updating personal information:

A client may seek to update their *information* held by us by contacting the Corporation's **Privacy Officer** at any time during office hours Monday to Friday.

The Privacy Principles require us to not store *information* longer than necessary. In particular, the Health Privacy Principles impose certain obligations about the length of time health records must be stored. You have the right to check what *information* we hold about you.

Under the *Victorian Privacy and Data Protection Act* the *Commonwealth Privacy Act* and the *Health Records Act*, an individual has the right to obtain access to *information* which the Corporation holds about them and to advise the Corporation of any perceived inaccuracy. There are some exceptions to this right set out in the applicable legislation. To make a request to access any *information* the Corporation holds about you, please contact the **Privacy Officer** in writing.

The Corporation may require you to verify your identity and specify what *information* you require. Although no fee will be charged for accessing your *personal information* or making a correction, the Corporation may charge a fee to retrieve and copy any material. If the *information* sought is extensive, you will be advised of the likely cost in advance.

Use of Identifiers:

We will assign employees and those who access our services or programs a unique identifier in the form of a staff or client ID number. These number/s are considered to be *personal information* and will be handled accordingly.

Except to the extent permitted by law, we will not use Commonwealth or State government identifiers (such as tax file numbers, Medicare number etc.) as our own identifiers nor will we disclose such identifiers, except where required or permitted by law.

What happens if the service closes or I move to another location?

Should a health service close down, or is sold or transferred and the provider is no longer there, current or former patients will be notified via a public notice. This notice would also be on display at the practice and letters to current patients sent out.

When a patient moves to another location or transfers to another provider, the Corporation will upon written request, make their *information* available to the other health service provider. To make a request for your *health information* to be transferred to another provider please contact the **Privacy Officer**.

Enquiries and privacy complaints:

Further information about the way the Corporation manages the *information* it holds, please contact the Corporation's **Privacy Officer**. If you have any concerns, complaints or you think there has been a breach of privacy, then also contact the Corporation's **Privacy Officer**.

If you are not satisfied with our response to your complaint you can refer your complaint to one of the following:

Privacy issues

Office of the Victorian Information Commissioner (OVIC)

- web site: www.ovic.vic.gov.au
- phone: 1300 006 842

Or

Office of the Australian Information Commissioner

- Web site: <https://www.oaic.gov.au/>
- Phone: 1300 363 992

Medical or Health related issues

Health Complaints Commissioner

- Web site: <https://hcc.vic.gov.au/>
- Phone: 1300 582 113