

PRIVACY POLICY

Purpose

This policy outlines how Murray PHN complies with the Australian Privacy Principles and relevant legislation dealing with privacy of Personal Information in Australia. It is intended to give individuals a better and more complete understanding of the sort of Personal Information that Murray PHN holds, and the way we handle that information.

It is also intended to provide details of how individuals can complain or report a breach of our responsibilities regarding privacy, and how we will handle such complaints.

Scope

This policy applies to all situations in which Murray PHN collects, holds, uses and discloses personal information.

Information collected and held by Murray PHN that is used for program reporting, and to support the review and improvement of services is de-identified and aggregated to a level which does not allow Murray PHN to identify the individuals.

Background

There are 13 Australian Privacy Principles that govern standards, rights and obligations around:

- the collection, use and disclosure of personal information
- an organisation or agency's governance and accountability
- integrity and correction of personal information
- the rights of individuals to access their personal information.

Definitions

Term	Definition
Consent	Means express or implied consent.
Health information	Includes: <ul style="list-style-type: none"> • Personal Information or opinion (e.g. a medical opinion) which is about the health, illness, disability or injury of an individual, or an individual's expressed wishes about the



	<p>future provision of health services to him or her, or a health service provided, or to be provided, to an individual.</p> <ul style="list-style-type: none"> • Other Personal Information collected to provide, or in providing, a health service to an individual. • Other Personal Information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances. • Genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.
Personal information	<p>Means information or an opinion means information or an opinion about an identified individual, or an individual who is reasonably identifiable:</p> <ul style="list-style-type: none"> • whether the information or opinion is true or not; and • whether the information or opinion is recorded in a material form or not. <p>Personal Information is information about an individual, natural person. Information on companies or other legal entities is not Personal Information. Personal Information includes Sensitive Information and Health Information.</p>
Sensitive information	<p>Is:</p> <ul style="list-style-type: none"> • Personal Information about an individual's racial origin, ethnic origin, political opinions, membership of a political association, religious belief or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation, sexual practices or criminal record; • Health Information; • Genetic information about an individual that is not otherwise Health Information; • biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or • biometric templates.

Any definition must be consistent with Murray PHN overall data dictionary, any additional terms defined by this policy must be added to the company wide dictionary maintained by the Senior Manager Information Assets. See [data dictionary](#) for existing defined terms.

Policy Statement

We respect people's Personal Information and their right to privacy. Protecting privacy when handling Personal Information is very important to Murray PHN and is fundamental to the way that we operate. When we collect personal information, it imposes a serious responsibility upon us to protect that information and maintain the trust that has been given to us.

1. Murray PHN's collection of Personal Information regarding an individual is performed and managed in accordance with the Australian Privacy Principles. Murray PHN will only collect information when it is necessary for its functions and activities.
2. Murray PHN will only collect Personal Information about an individual for the purposes of employment or arranging services and will only do so in a lawful and fair manner, with consent of the individual.
3. All Personal Information collected about an individual will be stored in appropriate Murray PHN systems and the privacy of their information will be protected through appropriate security measures.
4. Murray PHN will, through contractual agreements, require that all third-party entities that are involved in the provisioning of services must also adhere to Australian Privacy law and the Australian Privacy Principles.

5. Any Personal Information that is received unsolicited and identified by Murray PHN in the course of commissioning services, will be immediately destroyed and Murray PHN will notify the organisation that sent this information as soon as is practicable.
6. Any breaches of this policy will be handled in accordance with Murray PHN's Code of Conduct. Data breaches will be handled in accordance with Murray PHN's Data Governance Framework and Data Breach Response Plan.
7. Personal and Sensitive information will only be released in accordance with the Privacy Act and the Australian Privacy Principles where it is required for the provision of services to an individual or is mandatory under law.

The Privacy Act 1988 is an Australian law that is designed to protect and promote individual privacy and regulate how certain organisations, including government agencies and business with an annual turnover of more than \$3M, handle Personal Information. This law has the following principles that govern the collection, use, storage and disclosure of Personal Information in both the public and private sectors:

Australian Privacy Principles	Definition
APP 1 – Open and transparent management of personal information	Ensures that APP entities manage personal information in an open and transparent way
APP2 – Anonymity and pseudonymity	Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym.
APP 3 – Collection of solicited personal information	Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of sensitive information.
APP 4- Dealing with unsolicited personal information	Outlines how APP entities must deal with unsolicited personal information.
APP 5 – Notification of the collection of personal information	Outlines when and in what circumstances an APP entity that collects personal information must tell an individual about certain matters
APP 6 – Use or disclosure of personal information	Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.
APP 7 – Direct marketing	An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.
APP 8 – Cross-border disclosure of personal information	Outlines the steps an APP entity must take to protect personal information before it is disclosed.
APP 9 – Adoption, use or disclosure of government related identifiers	Outlines the limited circumstances when an organisation may adopt a government-related identifier of an individual as its own identifier or use or disclose a government related identifier of an individual.
APP 10 – Quality of personal information	An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up-to-date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up-to-date, complete and relevant, having regard to the purpose of the use or disclosure.
APP 11 – Security of personal information	An APP entity must take reasonable steps to protect personal information it holds from misuse, interference or loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.
APP 12 – Access to personal information	Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

Murray PHN Administration of Privacy information

1.1 What types of information do we collect and store?

In the ordinary course of business, we collect and hold many different types of Personal Information, from different stakeholders including consumers, carers, general practice, specialists, allied health professionals, job applicants, consultants, contractors, volunteers, students on placement, and members. These types of Personal Information typically include:

- an individual's name, signature, address, phone number or date of both; dietary information for catering (where applicable);
- training records and competency assessments;
- health practitioner registration details;
- participation in continuing professional development (CPD);
- sensitive information such as relevant professional memberships and affiliations;
- relevant qualifications and accreditation;
- special interests;
- attendance at events, photos and/or videos taken at events or by closed-circuit television cameras ("CCTV");
- access to and use of our services;
- bank account details;
- communication history; and
- browsing history accessing our website or resources.

Additionally, and from time to time we made need to collect health information / sensitive information about individuals access to care, if this is relevant / necessary for Murray PHNs activities in enabling referrals and supporting access to health services

Where an individual visits our website, we collect and store information such as individual IP addresses, internet service providers, activity on our website such as pages viewed and the information downloaded, the page from where the individual visited our website, the type of browser used and unique device identifiers. This information is usually anonymous, and we do not use it to identify individuals. However, due to the nature of internet protocols, such information might contain details that identify individuals. This information is only used to improve our website and related services.

We may also collect Personal Information in other ways, however, we only do this where it is reasonably necessary for our functions and activities. Where reasonable Murray PHN will inform individuals at or before the point of collecting information or ensure that the individuals are aware of the collection.

We may also collect de-identified information from third parties who we work with and/or who receive funding from us such as commissioned service providers and health clinics.

1.2 How do we collect and hold that information?

It is our practice to collect Personal Information directly from the individual or their authorised representative, unless it is unreasonable or impracticable to do so.

Sometimes we collect Personal Information from a third party or a publicly available source, usually where the individual has Consented to such collection or would reasonably expect us to collect their Personal Information in this way, or in other instances where it is necessary for a specific purpose such as the investigation of a privacy complaint.

In limited circumstances we may receive Personal Information about individuals from third parties who contact us and supply us with the Personal Information of others in the documents they provide to us.

In circumstances where it is not impractical to deal with individuals who have not identified themselves or have used a pseudonym, and if it's not required or authorised by law to deal with identified individuals, individuals have the right to anonymity or pseudonymity when providing information.

1.3 Why do we collect, hold, use and disclose personal information?

We primarily collect Personal Information for our functions and activities that are set out in the Murray PHN Strategic Plan and the Murray PHN Constitution. Our key objectives are to increase the efficiency and effectiveness of health services for patients, particularly those at risk of poor health outcomes, and improving co-ordination of care to ensure patients receive the right care in the right place at the right time. We also collect Personal Information for objectives that are reasonably necessary for, or which are directly related to one or more of our functions or activities or are otherwise authorised or required by law.

We may disclose information to other agencies or partners if it will assist them in contributing to the achievement of our objectives. We do not ordinarily give Personal Information to government agencies, organisations or anyone else unless one of the following applies, this includes:

- providing advice, treatment, referrals, or follow-up communications to individuals or their representatives;
- coordinating event logistics, including sharing registration and relevant dietary information with third parties (e.g. venues or caterers);
- conducting program evaluations, satisfaction surveys, and service outcome reviews, including following up with individuals, families, or referring parties;
- the individual has Consented.
- we are obligated under any agreement we have with a government agency or like organisation, such as for audit, review, evaluation, accountability, insurance or other purposes.
- the individual would reasonably expect, or has been told, that information of that kind is usually passed to those individuals, bodies or agencies.
- it is otherwise required or authorised by law or court order, or other governmental order or process, such as where we believe in good faith that the law compels us to disclose information to:
 - lessen or prevent a serious threat to your life, health or safety or public health or safety, where it is impractical to obtain your consent;
 - take appropriate action in relation to suspected unlawful activity or serious misconduct;
 - to assert a legal or equitable claim.

it is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of public revenue.

We may also collect, use and disclose aggregated and de-identified data with other Primary Health Networks, government bodies (both state and federal level) and third parties. This information is used to support planning, review and improvement of Murray PHN services, funding applications, and the development of programs that address identified community health needs.

When we temporarily provide Personal Information to companies who perform services for us, such as specialist information technology companies, mail houses or other contractors, we require those companies to protect your Personal Information in accordance with the Australian Privacy Principles.

Personal Information will not be disclosed to overseas recipients, except in limited situations where we have engaged information technology service providers and they provide services such as cloud services to store or back up Personal Information. In these circumstances the service providers are contractually bound by this Policy and must comply with the Australian Privacy Principles and other applicable privacy

laws. Otherwise, we do not disclose or allow a third party located outside Australia to access the Personal Information we hold.

1.4 Direct Marketing

On occasion we may use the Personal Information we collect from you to identify services or events which we believe may be of interest to you. We may then contact you to let you know about these and how they may benefit you. We will generally only do this with your consent, and we will always give you a choice to opt out of receiving such information in future.

1.5 How can people access the information that we hold about them, and how can they correct or amend such information?

We take steps to ensure that the Personal Information we collect is accurate, up to date and complete. These steps include maintaining and updating Personal Information when we are advised by individuals that their Personal Information has changed, and at other times as necessary.

It is inevitable that some Personal Information which we hold will become out of date. We will take reasonable steps to ensure that the Personal Information which we hold remains accurate and, if you advise us of a change of details, we will amend our records accordingly.

If we do not agree to make requested changes to Personal Information the individual may make a statement about the requested changes and we will attach this to the record.

Individuals can obtain access to the Personal Information which is held about them by contacting any of our offices throughout the region. In the case of Sensitive Information (including Health Information), your request should be directed to the Chief Corporate Officer who is Murray PHN's nominated Privacy Officer. We reserve the right to refuse access where an exception applies, for example, where releasing the information would unreasonably impact the privacy of another individual. Alternatively, we reserve the right to redact the information made available, to protect the privacy of other individuals. We also reserve the right to verify the identity of the person requesting the information and their entitlement to access it.

1.6 How can people complain about a breach of privacy, and how will we deal with such complaints?

If you believe that there has been a breach of this policy, you should set out details of your complaint and send it to privacy@murrayphn.org.au or addressed to the Privacy Officer at 3-5 View Point, Bendigo, VIC, 3550.

Complaints which are received will be resolved in accordance with Murray PHN's complaints handling procedures. Complaints will normally be investigated and either resolved or progress communicated to the complainant within 30 days.

We reserve the right to verify the identity of the individual making the complaint and to seek further information from the complainant about the circumstances of the complaint. We reserve the right to refuse to investigate or to otherwise deal with a complaint where permitted under the Privacy Act 1988 (Cth). For example, we may refuse to investigate or to otherwise deal with a complaint if we consider the complaint to be vexatious or frivolous.

If you are not satisfied with our response to your complaint, or you consider that we may have breached the APPs or the Privacy Act 1988 (Cth), you can make a complaint to the Office of the Australian Information Commissioner ("OAIC").

Office of the Australian Information Commissioner

Postal address: GPO Box 5288 Sydney NSW 2001

Phone: 1300 363 992

Email: foi@oaic.gov.au

Website: www.oaic.gov.au

1.7 Security of information held

Murray PHN is committed to keeping your trust by protecting and securing your Personal Information. We employ appropriate technical, administrative and physical procedures to protect Personal Information from unauthorised disclosure, loss, misuse or alteration.

We limit access to Personal Information to individuals with a business need, consistent with the reason the information was provided. We keep Personal Information only for as long as it is reasonably necessary for the business purposes or otherwise as required by the law.

Responsibilities

Privacy Officer

The Privacy Officer is required to:

- provide internal privacy advice involving the handling of personal information, or in response to ad-hoc enquiries from employees about how they should handle personal information.
- Responding, or assisting Murray PHN to respond to queries about our privacy practices from members of the public.
- Handling and investigating privacy issues and complaints
- Assessing whether requests from other organisations to share personal information that is held by Murray PHN is permitted under privacy law.

All Staff

- All staff must comply with Privacy Law and the Australian Privacy Principles when dealing with Personal and Sensitive information regarding members of the public to whom Murray PHN provides or provisions services.

Relevant Legislation

Privacy Act 1988

Australian Privacy Principles

Document Control

This document will be reviewed every two years and approved by the Board.

Date	Author	Modification	Version
7/8/2015	Bruce Baehnisch	Migrated from iLocal	1.0
10/5/2016	Bruce Baehnisch	Rebranded	1.1

8/5/2017	Bruce Baehnisch	Updated Strategic Goals, Locations and added details of notifiable data breaches. Update to Appendix 2.	2.0
15/2/2018	Darryn Young, Governance Lead	Update for Notifiable Data Breach legislation, addition of Appendix 4.	2.1
Oct 2019	Darryn Young, Governance Lead	Update to incorporate recommended changes from legal firm Russell Kennedy – Appendices 2 and 3 themes incorporated into main policy document, with website statement to appear on website and Appendix 4 extracted into separate Data Breach Response procedure.	3
October 2020	Darryn Young, Governance Lead	Related documents updated	3.1
November 2021	Darryn Young, Governance Lead/Board Secretary	Position Titles updated	3.2
24 September 2025	Will Gwosdz, Manager Governance	<ol style="list-style-type: none"> 1. Put policy on new template. 2. Minor modifications to Definitions table. 3. Addition of minor information for “What types of information do we collect and store. 4. Minor adjustments in structure for better alignment with Australian Privacy Principles and its definitions. 5. Moved guidance information to Guidelines document. 6. Reviewed and updated by Russell Kennedy. 7. Addition of Clause 1.8 after receipt from Russell Kennedy and a gap identified with Intellectual Property. 	3.3