

Darling Downs and West Moreton PHN

Corporate Policy

Policy name:	Privacy Policy
Approved by:	Board
Date Effective:	1/07/2026
Review Date:	30 June 2027
Reference Number:	V3.0
Document Classification:	Public

Summary of Revisions

Date of changes	Summary description of changes made	Revised by (role)	Approved by (role)
July 2020	V1.0 Development and approval of new policy	ED S&O	CEO
February 2022	V1.1 New Template and Review	ED S&O	ED S&O
August 2023	V1.2 Review and update	ED S&O	Board
January 2025	V.1.2.1 Updated frequency of review period	Privacy officer	ED S&O
September 2025	V2.0 New Template and Review	ISMS team	ED S&O
June 2026	V3.0 Review and update	ISMS team	ED S&O

Table of Contents

Policy statement	4
Objective of this Policy	4
Protecting your privacy	4
Definitions	4
Why we collect information	6
What personal information we collect	6
Exception in relation to employee records	8
Collection of Sensitive Information	8
Direct and indirect collection	8
De-identified and Aggregated Data	8
Anonymity and Pseudonymity	9
Unsolicited information	9
Direct marketing	9
Disclosure of personal information	9
Overseas disclosure	9
Use of Technology Tools	9
Access and correction	9
Response to access requests	10
Response to correction requests	10
Third party sites	10
Cookies	10
Security and accuracy	10
Accuracy	11
Retention and Deletion	11
Data Breaches	11
Complaints	11
Contact Us	11
Related policies and documents	12

Policy statement

This Privacy Policy sets out how Darling Downs and West Moreton Primary Health Network (the PHN) Limited (ABN 51 605 975 602) manages personal information provided to or collected by it. Along with our Privacy Collection Statements, our Privacy Policy lays down the principles by which we collect, store, use and disclose any personal information provided to us, or collected from other sources.

Objective of this Policy

The objective of this policy is to inform members of our community, providers, stakeholders, funders, and anyone else whose personal information is collected, stored, used, or disclosed by the PHN about how:

- we protect their information
- individuals can access and correct the personal information we hold about them
- individuals can make a complaint or ask a related question.

Protecting your privacy

Darling Downs and West Moreton PHN (the PHN) takes the protection of your personal information very seriously. We are committed to ensuring that your personal and health information is handled in accordance with our legal and contractual obligations, maintaining a consistent approach to privacy across all levels of our organisation.

The PHN complies with the [Australian Privacy Principles](#) (APP) under the [Privacy Act 1988 \(Cth\)](#). This commitment extends to all staff and volunteers, ensuring that every individual representing our organisation handles personal and health information with the highest level of integrity and legal compliance.

We regularly review our policies and procedures regarding personal information and may update this Privacy Policy from time to time. Any changes to this Privacy Policy will be published on our website or can otherwise be obtained by contacting us and requesting a copy. We understand that you may have concerns about your privacy and confidentiality of personal information shared with us. If you have any questions or concerns, please email us at privacy@ddwmpnh.com.au.

Definitions

The following terms have the meaning as set out below:

Term	Definition
Darling Down and West Moreton PHN or the PHN or 'us' or 'we'	Darling Downs and West Moreton Primary Health Network Limited ABN 51 605 975 602 and all related entities and affiliates.
Commissioned Service Provider	An external organisation or practitioner contracted by the PHN to deliver specific health services, bridging gaps in local care.
Consent	Consent has the following key elements: • voluntary, informed, current, specific and unambiguous • the individual must have the capacity to understand and communicate their consent • the consent can be easily withdrawn.

Privacy Policy

Term	Definition
Cookie	A small file stored on your device that allows our website to recognise your browser and remember certain information, such as your preferences or previous visits, and which store and sometimes track information about your use of our website.
De-identified information	Information that no longer identifies an individual or where an individual is no longer reasonably identifiable. De-identification generally involves two steps: 1. removing personal identifiers, such as a person's name, address, date of birth, or other identifying details. 2. removing or altering other information that could allow someone to be identified, for example due to a unique characteristic or a combination of information that could enable re-identification For further guidance, visit the OAIC's page on De-identification and the Privacy Act.
Health information	Any personal information about the health or disability of an individual. Health information is considered Sensitive Information
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable. This applies whether the information or opinion is true or not, and whether it is recorded in a material form or not. The Privacy Act recognises a broad range of information as personal information, including Sensitive Information and Health Information: For more information, visit the OAIC's page on What is personal information?
Privacy Act	Privacy Act 1988 (Cth) as amended and updated from time to time.
Sensitive information	Personal information that includes information or an opinion about an individual's: • racial or ethnic origin • political opinions or associations • religious or philosophical beliefs • trade union membership or associations • sexual orientation or practices • criminal record • health or genetic information • some aspects of biometric information. For more information, visit the OAIC's page on What is sensitive information?
Stakeholder(s)	Anyone external to the PHN that has a relationship with the PHN including but not limited to commissioned service providers, advisory committee members, stakeholder working groups, the community and tender panel members.
OAIC	Office of the Australian Information Commissioner
NDB	The OAIC under the Federal Notifiable Data Breaches (NDB) scheme. Must notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved.

Why we collect information

The PHN's primary function is to assess and understand the health needs of the local region and to engage service providers to provide health services within the local region. This may include:

- commissioning and co-ordinating health and community services
- supporting General Practices including:
 - providing reports, advice and feedback on quality improvement and other Practice improvement areas for General Practices via reports, phone calls, emails, in-person meetings and other forms of communication
 - generating, processing and submitting data for State or Commonwealth Government programs for which the Practice is enrolled or obligated to participate, such as the Practice Incentive Program for Quality Improvement (PIP QI)
 - providing reports, alerts and notifications via shared software
- undertaking population health research and analysis, planning, development, monitoring, evaluation and other statistical analysis and research intended to improve community health outcomes, including through data linkage and data comparison activities, and publication of any results
- evaluation, monitoring and service improvement of service providers
- stakeholder and relationship management including surveys, training and events
- sharing information with federal, state and local government agencies, local health districts and health service providers, where authorised, including the creation and sharing of Aggregated Data to support planning, development and evaluation of health policy and programs, including health workforce policy and programs
- collaboration with other Primary Health Networks to support any of the functions or purposes listed in this section
- management, improvement and optimisation of the PHN and its services including provision of an enhanced and more personalised experience for people when dealing with the PHN, whether interacting via website or other online services and in person services, and for security and quality purposes.

We only collect personal information that is reasonably necessary for, or directly related to, one of these identified functions and activities, and any additional functions and activities as may be notified from time to time.

We will only use personal information for the purpose for which it is collected or for a directly related secondary purpose that you would expect your personal information to be used for (unless legally required or authorised to do otherwise).

What personal information we collect

The kinds of personal information that the PHN collects will vary depending on our particular interaction or dealing with you, and the purpose for which we are collecting your personal information.

The types of personal information we collect and the purpose for collecting that information, is described below:

Category of Personal Information Collected	Purpose of collection
Contact details via online forms or phone calls including name, email address and phone number	• Respond to your queries • Provide you with services, unless you tell us otherwise • Determine your eligibility for services we provide • Maintain our relationship with you

Privacy Policy

Category of Personal Information Collected	Purpose of collection
Information from General Practices Note: Patient information received from General Practices is De-identified before it is shared with the PHN.	- Population health research - Quality improvement feedback for General Practices, - Generating, processing and submitting data for State or Commonwealth Government programs for which the Practice is enrolled or obligated to participate, such as the Practice Incentive Program for Quality Improvement - Creation of Aggregate Data for use in policy and planning and in collaboration with other PHNs, agencies and health service providers
Information about Primary Care Providers including details of practice and health care provider information	- Reporting purposes - Stakeholder engagement and relationship management - Disaster management
Information to meet funding partner requirements including diagnosis subject to treatment and information relating to age, ethnicity and social situation	- Reporting purposes including reporting to Funding Partners - Meet our responsibilities to Funding Partners
Event, training and educational program registration details including name and email address, phone number, professional role and qualification details	- Enable participation in events, training and educational programs and other engagement activities - Sharing with event, training and educational partners to record and confirm participation and/or completion, and as otherwise required for professional certification, credentialing and professional development purposes
Marketing/ subscriptions details including name and email address, phone number, professional role, and Local Government Area	- Issue relevant newsletters, updates and other online information - Provide you with information about our services (unless you tell us you do not want to receive this information)
Surveys and research details including name and email address, your IP address and the type of browser or device you used and any personal information you disclose in response to a survey. <i>Note: Participation in survey and research is voluntary. Where possible, survey responses will be collected and reported in a de-identified or aggregated form.</i>	Administer surveys and gather feedback, including: - as part of our population health research and analysis - to evaluate and improve our services and service providers, community engagement and funding - to evaluate and improve events, training and educational programs and other engagement activities.
Web browsing details include your IP address, the date, time and duration of your visit, the pages you accessed and the documents you downloaded, the type of browser or device you used, the website that referred you to ours and what	- Website management, improvement and optimisation including provision of enhanced and more personalised experience when interacting with the website - Security and quality assurance <i>Note: This information is collected using web logs and analytics tools. We do not use it to identify individuals unless it is necessary for the</i>

Privacy Policy

Category of Personal Information Collected	Purpose of collection
country and what systems are used to access the site.	<i>investigation of a security incident, technical fault, or where it is otherwise required or authorised by law.</i>

There is no legal requirement for you to provide your personal information, however if you choose not to disclose your personal information this may impact our ability to deliver our services and programs and meet our Stakeholder needs.

Exception in relation to employee records

In accordance with the Privacy Act 1988 (Cth), the APP do not apply to employee records where there is a direct relationship between us and a current or former employee. Consequently, this Privacy Policy does not apply to our handling of information that falls within this employee records exemption.

Collection of Sensitive Information

As part of the provision of primary healthcare services and for the purpose of understanding our region's health needs particularly in relation to vulnerable populations we may collect Sensitive Information that includes information about people from Multicultural backgrounds, people living with a disability, people from the LGBTIQA+ communities and Aboriginal and/or Torres Strait Islander peoples.

We will only collect Sensitive Information, such as health or ethnic background information, with your consent unless we are otherwise authorised or required by law to do so.

Direct and indirect collection

We collect information by lawful and fair means directly from you, or from third parties if it is unreasonable or impracticable to collect it from you.

In some cases, the law allows us to collect information from other sources without your consent. For example, we collect health information from third parties such as hospitals, general practitioners and other health service providers pursuant to legal provisions and usually subject to data sharing agreements that clearly identify the data to be shared and the use of that data.

You can ask your health service provider not to share your personal information with us.

We may also collect personal information from public sources (e.g., national health practitioner register, internet), or through memberships (e.g., with peak bodies or accreditation agencies), to understand compliance against standards or population health needs.

De-identified and Aggregated Data

Wherever possible data shared with us by third parties such as hospitals, general practitioners and other health service providers (including Commissioned Service Providers) is de-identified before sharing in accordance with approved protocols. We have policies and procedures in place to minimise the risk of re-identification of any shared De-identified Data.

De-identified information helps us understand how health services are delivered, how well they are performing, and what future health needs may exist in our community.

As well as using that de-identification information for the purposes listed above, we may also aggregate details from that data to support reporting, policy and planning and agreements with other Stakeholders including funding partners. Aggregate data does not include any personal information and cannot be used (alone or with other reasonably available information) to reasonably identify any individual. Aggregate data does not include any personal information and cannot be used (alone or with other reasonably available information) to reasonably identify any individual.

Privacy Policy

Anonymity and Pseudonymity

Where it is lawful and practical, you can choose to interact with us anonymously or by using a pseudonym. This means you do not have to identify yourself unless it is necessary for us to provide a service or meet our legal obligations. For example, if you call us to ask a general question, you can choose not to give your name. If you complete a survey or contact us by email, you may choose to use a pseudonym, such as a nickname instead of your full name.

Unsolicited information

Unsolicited information is information that we have not asked for. If we receive any unsolicited information that is not reasonably necessary or directly related to one or more of our business activities, then we will de-identify or secure destroy it as soon as practicable.

Direct marketing

We will only use or disclose your personal information for direct marketing purpose with your consent. You can opt out of receiving direct marketing communications from us by contacting us or unsubscribing from the service or emails. Your request will be processed within five business days in line with the Spam Act 2003 (Cth).

Disclosure of personal information

We are authorised by law to disclose your personal information to third parties in certain circumstances, or in the interests of your health and safety. For example, we provide information to the Australian Government and other State government agencies and to health service providers as part of our obligations as a Primary Health Network.

Otherwise, we will only disclose your personal information to third parties for the purpose for which is collected or a directly related and reasonably expected secondary purpose and, where required, with your consent,

Where possible, we only disclose De-identified Information to third parties where the personal information is essential for the business activity.

Overseas disclosure

We do not disclose your personal information overseas other than when we share with administrative support providers. This might include sharing contact details and other personal information with event and training partners and third-party marketing support providers, which may store and process that information outside of Australia including in the United States. We always take reasonable steps to ensure that your personal information will be properly protected by any third party we engage. We will let you know if we otherwise disclose your personal information overseas, including details of the relevant country.

Use of Technology Tools

We do not use automated tools to make decisions which may have a significant impact on any individual. We may use technology tools, including artificial intelligence-assisted tools to support activities such as research, analysis, drafting and administrative functions. Where these tools process personal information, appropriate contractual, governance, security, legal and human oversight controls are in place.

Access and correction

You may request access to or the correction of your personal information by contacting us using the details provided in the "Contact Us" section of this policy.

Privacy Policy

Please include enough detail for us to identify you and locate the relevant information. To protect your privacy, we may need to verify your identity before providing access to or correcting your information.

We will respond to your request within a reasonable period (usually 30 days).

Response to access requests

In most cases, we will provide you with access to your personal information upon request. While we will not charge you for making a request, we may charge a reasonable fee to cover the cost of providing access (such as staff time for locating and retrieving information or costs of photocopying and postage). If a fee applies, we will notify you of the estimated cost and seek your agreement before proceeding with your request.

We may decline a request for access in circumstances prescribed by the Privacy Act 1988 (Cth). If we refuse access, we will provide a written notice setting out the reasons for the refusal (unless it would be unreasonable to do so) and information regarding your options, including how to make a complaint.

Response to correction requests

On receipt of your request, we will take reasonable steps to correct the information so that it is accurate, complete and up to date.

If we refuse to correct your personal information, we will provide you with a written notice that set out the reasons for our refusal (unless it would be unreasonable to provide those reasons), together with details regarding the mechanisms available to you to make a complaint.

You may also request that we include a note on your file that records your request for correction to your information and may request that we notify third parties to whom we have disclosed personal information of any correction.

Third party sites

Our website or online communications may contain links to other websites or information. Please note that we do not have control over these external sites and are not responsible for their privacy practices. Please be aware that information handling of a linked website or service might not be the same as ours and you should refer to the relevant privacy policy of that third party for more information.

Cookies

Our website uses Cookies to improve your browsing experience and make our online services easier to use. We do not use Cookies to track your browsing activity across other websites. You can choose to disable cookies or adjust your browser settings to notify you when cookies are used. However, some parts of our website may not function properly if cookies are disabled.

Security and accuracy

The PHN takes the security of your personal information seriously. The PHN takes reasonable measures, proportional to the associated risk, to protect personal information it holds from loss, misuse, unauthorised access or disclosure, alteration and destruction.

Information will be held in a variety of ways, including in paper and electronic format, on secure databases that are only accessible by relevant employees. The PHN may also hold photographic images taken of you on a secure database.

Privacy Policy

Accuracy

The PHN shall take all reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete and, where necessary, appropriately updated.

Retention and Deletion

Pursuant to its records retention policies and procedures, the PHN shall not keep personal data for longer than necessary or permitted by law.

Data Breaches

If a data breach occurs involving your personal information, the PHN will notify you and the OAIC in accordance with the NDB scheme. We will also take all reasonable steps to contain the incident, mitigate any potential harm, and support you with information to help protect your privacy.

For any critical incidents, including data breaches, that impact any of our Commissioned Service Providers, please contact your Commissioning Coordinator or submit details on our [Critical Incident Report Form](#).

Complaints

Any complaints or concerns about how the PHN handles personal information can be sent to our Privacy Officer at privacy@ddwmpnh.com.au. The PHN will respond to any complaint or concern within 30 days of the complaint or concern being received.

If an individual believes the complaint has not been appropriately handled by the PHN, they should contact the Office of the Australian Information Commissioner using their online Privacy Complaint Form at www.oaic.gov.au

Contact Us

The PHN welcomes your feedback on this Privacy Policy. If you have any questions about the policy or if you are an individual seeking access to, or correction of, your personal or health information held by the PHN, please contact our Privacy Officer by:

Email: privacy@ddwmpnh.com.au

Phone: [07 4615 0900](tel:0746150900) during business hours, Monday to Friday.

Darling Downs Office	Level 1, 162 Hume Street (PO Box 81), Toowoomba QLD 4350
West Moreton Office	Level 5, World Knowledge Centre, 37 Sinnathamby Boulevard, Springfield Central QLD 4300

Related policies and documents

- *PHN Privacy Statement*
- *Privacy Act 1988 (Cth)*
- *Australian Privacy Principles*
- *Privacy and Other Legislation Amendment Act 2024 (Cth)*
- *Data Governance and Information Security Policy*
- *Information Security Incident Management Plan*
- *Record Management Policy*
- *Password Policy*
- *Personal Information Protection Guidelines*
- *Confidentiality Deed*
- *Notifiable Data Breach Scheme*
- *Information and Data Request Form*