Privacy policy

Policy name:	Privacy policy
Date approved:	18 February 2025
Next revision:	1 April 2026
Approved by:	Chief Executive Officer
Organisation contact:	Team Leader | Data

Purpose

The purpose of this policy is to ensure a consistent approach to privacy and that all staff of Brisbane North PHN handle personal information in accordance with the *Privacy Act 1988 (Cth) (as amended)* and the Australian Privacy Principles.

The PHN is committed to ensuring PHN Information systems are secure and protected from Information Security threats whether internal or external, deliberate or accidental. Brisbane North PHN Information Security Management System is ISO27001:2013 accredited.

Related documents

This policy is to be read in conjunction with:

- PHN Privacy Statement
- Privacy Act 1988 (Cth)
- Australian Privacy Principles
- Data Governance Framework
- Information Security
- Information Management
- Data Breach Response Plan

Responsibility

It is the responsibility of all staff to manage personal and sensitive information in accordance with the Act, our Privacy Policy and Privacy Statement. The Lead | Data Governance & Insights is responsible for the continued development of this policy and is the designated Privacy Officer.

Changes to the policy will be made with the approval of the Chief Executive Officer.

Privacy

The Privacy Act 1988 (Cth) applies to the Brisbane North PHN. The Act protects personal and sensitive information, particularly health information. Our Privacy Statement is based on the Australian Privacy Principles and outlines how we collect handle and store personal information.

Every employee's contract of employment acknowledges their privacy obligations and confidentiality requirements under the Act.

Personal information

Personal information is information or an opinion about an identified individual or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not.

Personal information collected by the organisation generally comprises name, address, date of birth, gender, occupation, employer, contact details (including telephone, facsimile and e-mail), and qualifications. Sometimes we collect **sensitive information** that might include information or an opinion about cultural ethnic origin, health or medical information, membership of a political association, professional or trade association and financial information. We may also collect photographs, videos, and other recordings of you where those assist us in providing you with services

Records directly relating to a current or former employment relationship are exempt in the Act.

Request for Personal Information

Under no circumstances is a staff member permitted to disclose personal information without first contacting the Privacy Officer (Lead | Data Governance & Insights). In some circumstances under the Act or by legal request we have an obligation to disclose certain personal information but in every instance the Privacy Officer (Lead | Data Governance & Insights) must be informed.

Notifiable data breach

Under the Act the organisation has an obligation to investigate, assess and respond to any data breach. Under the Act and the Notifiable Data Breach Scheme we have an obligation to report the incident and the outcome to the Office of the Australian Information Commissioner.

A data breach occurs when personal information is subject to unauthorised access or disclosure or is lost.

All staff have a responsibility to follow the Data Breach Response Plan in the event of an actual or suspected data breach.

Reporting a breach

If a staff member becomes aware of a breach, they must follow the Data Breach Policy and complete the Data Breach Response form.

Due to the sensitivity and nature of some data breaches, the organisation recognises that this has the potential to cause some distress to staff involved. If you are experiencing distress through the result of the data breach/potential data breach, please reach out to your manager, the privacy officer or people and culture team to discuss strategies and support available to you.

Receiving a privacy complaint

If a staff member receives a privacy complaint, they should record the contact details of the complainant, nature and circumstance of the privacy breach and forward the details to our Privacy Officer (Lead | Data Governance & Insights). On receiving this information, the Privacy Officer will inform the CEO and contact the parties involved to investigate and resolve the complaint.

Australian Privacy Principles

Brisbane North PHN acknowledges and takes seriously its obligations under the Act, particularly the Australian Privacy Principles (APPs). They are found in Schedule 1 of the Act.

APP 1—Open and transparent management of personal information

To ensure personal information is managed in accordance with the legislation and with the Australian Privacy Principles, we have a number of policies and procedures to assist staff when handling personal information.

Our Privacy Statement details what, how, when and why we collect personal information and our Privacy Policy helps all staff understand the importance and how we apply the APPs.

Brisbane North PHN is ISO 9001:2015 certified and undertakes regular reviews of our policies and processes.

Our Privacy Statement is available in our employee handbook, on our website www.brisbanenorthphn.org.au, in our foyer or in writing on request.

Any complaints in relation to the handling of personal information are to follow the company complaints and feedback policy. In most cases, the complainant will be asked to lodge their complaint in writing.

Unless a complaint can be dealt with immediately to the satisfaction of both parties, the organisation will provide a written response to the complaint within 30 days of it being received.

If an individual believes their complaint has not been appropriately handled by the organisation then the individual can contact the Office of the Australian Information Commissioner, Privacy Hotline 1300 363 992 or at www.oaic.gov.au.

Individuals can request a copy of our Privacy Statement and we must take reasonable steps to provide it in the form they request.

APP 2—Anonymity and pseudonyms

Where it is lawful and practicable to do so, we give individuals the option of interacting anonymously. This may involve allocating individuals with a pseudonym. We accept anonymous enquiries where possible, and advise individuals that our website privacy page includes information on how to disable website cookies.

APP 3—Collection of solicited personal information

We collect personal information that is reasonably necessary for, or directly related to our functions and activities.

Sometimes we collect sensitive information from individuals in connection with an activity or service we provide.

We only collect information directly from the relevant individual, unless it is unreasonable or impractical to do so, or where otherwise required or authorised by law.

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

Information is collected so that we may:

- administer relationships
- answer queries
- provide an enhanced and more personalised experience when individuals deal with the organisation
- provide services, unless told otherwise
- provide information about our services, unless told otherwise
- determine an individual's eligibility for a service we provide
- make and receive payments.

Personal information must not be stored without consent. Consent can be secured verbally and can either be express or implied. For example, express consent is saying, "yes, I would like to be on your database" and implied consent is saying, "I would like to receive your newsletter every month".

In our internal client management system (ChilliDB) the Privacy Request 'No Contact' designation for an individual must not be removed until consent has been received. If an individual requests no further contact or wishes to unsubscribe from our contact or mailing lists then the 'No Contact' designation must be ticked.

It is important that we allow individuals to choose how they wish to receive information from us. Inclusion of a statement offering the option to opt-out from contact via one or all contact methods should be provided. Suggested wording can include "Please advise if any of the above contact details are not to be used for contact by the PHN". You can also opt not to provide a contact method or opt-out at any stage by contacting us.

When obtaining consent, staff must also ensure that the contact preferences of the individual are selected in ChilliDB, e.g. where it is stated by the contact that they request no contact by phone and/or email, this is recorded. In the instance that contacts are providing contact information, it is implied that this can be used by the organisation.

If sensitive (health) information is collected then more explicit consent is obtained from the individual that supports their enrolment in a service or program we might offer. In some cases, we will receive emergency referrals with sensitive information. This is permitted by the Act as a 'permitted general situation', but the information must ultimately be dealt with as unsolicited information (see below).

It is the responsibility of all staff to ensure that any hard copies of documents with personal or sensitive information are handled securely in accordance with our policies.

APP 4—Dealing with unsolicited personal information

If we receive unsolicited personal information and we can determine that we would have been permitted to collect that information under APP3, then APP5 to APP13 apply to that information.

If the unsolicited information could not have been collected under APP3 and the information is not contained in a Commonwealth record then we will destroy or de-identify that information as soon as practicable, but only if it is lawful to do so.

APP 5—Notification of the collection of personal information

We take reasonable steps in the circumstances to notify the individual or ensure that the individual is aware when we collect personal information and the purpose we collect the information for.

Unless legally required or authorised to do otherwise we obtain consent when collecting personal information about individuals.

We only collect personal information about an individual that is reasonably necessary for or directly related to our activities and relevant to the purpose for which it is collected.

APP 6—Use or disclosure of personal information

We only use personal information for the purpose for which it is collected, the primary purpose. We do not use or disclose the information for a secondary purpose unless: the individual has consented to the use; or the individual would reasonably expect us disclose the information and the information is directly related to the primary purpose; or required by law.

In certain circumstances where personal information may become known to our contractors, agents and outsourced service providers, confidentiality arrangements will be put in place. Contractors, agents and outsourced service providers are not able to use or disclose personal information for any purposes other than the original agreed intended purpose.

APP 7—Direct marketing

We use or disclose information about an individual for the purpose of promoting our services and programs:

- if we collected the information from the individual
- if the individual would reasonably expect us to use or disclose the information for that purpose.

We provide a simple means by which the individual may easily request not to receive direct marketing communications from us or unsubscribe. All requests to opt out or unsubscribe must be implemented promptly (see managing ChilliDB Privacy Request in APP3).

APP 8—Overseas disclosure of personal information

We store personal and sensitive information in Australia and do not presently disclose personal information overseas. As required by the Act, we will advise the individual if information is likely to be disclosed to a recipient in another country.

APP 9—Adoption, use or disclosure of government related identifiers

We do not adopt a government related identifier of an individual as our own identifier unless authorised by an Australian law or a court/tribunal order.

We do not use or disclose a government related identifier of an individual unless it is reasonably necessary for the organisation to verify the identity of the individual for the purposes of our activities and functions or unless authorised by an Australian law or a court/tribunal order as stated in APP9.

APP 10—Quality of personal information

It is the responsibility of all staff to take every reasonable step to keep the personal information we collect, use or disclose complete, current and accurate.

APP 11—Security of personal information

We use a number of systems to protect the personal information we keep from misuse, malicious attack, virus, loss, unauthorised access, modification or disclosure. The PHN has an Information Security Management System (ISMS) and follows the ISO27001 risk-based framework to manage the security of personal information. As part of our quality management processes, we regularly review our controls and policies to ensure they remain effective.

Computers automatically logout when not being used. Staff use strong passwords that are unique and not shared with others. Staff laptops and USB drives are encrypted to protect corporate information, VPN and Multifactor authentication is used when accessing PHN Information systems from outside the office network.

When disposing of any electronic devices that held electronic personal information, the devices or hard drives are rendered inoperable before the item can be disposed of.

Visitor access to the office is controlled and visitors will not have access to personal information.

We will take reasonable steps to destroy or de-identify personal information once the Organisation no longer needs it for any authorised purpose unless required by Australian law or a court/tribunal order to retain the information.

APP 12—Access to personal information

Individuals can request, in writing, access to their personal information. All such requests should be forwarded to our Privacy Officer. On receiving a valid written request, we will provide the individual a copy of the personal information held by us, unless legally required or authorised to do otherwise. If access is denied due to a particular circumstance permitted by the Privacy Act we will let the individual know in writing.

A small but reasonable administration fee may be levied to collate and provide the requested personal information.

We will respond to an individual's access request as soon as possible and will endeavour to comply within 15 business days.

APP 13—Correction of personal information

We will take reasonable steps to correct personal information we hold about an individual if the information is found to be inaccurate, out of date, incomplete, irrelevant or misleading.

Corrections can be instigated by us if we are satisfied the correction is necessary or an individual can request their personal information is corrected.

We will take reasonable steps to notify other APP entities if personal information provided by us has been corrected, unless impracticable or unlawful.

We will respond to an individual's correction request as soon as possible and will endeavour to comply within 15 business days. We will not charge an individual for the correction.

If we refuse to correct the personal information, we will give the individual written notice detailing the reasons and details of the mechanisms available to them to make a complaint. If requested, we must include a note of our refusal to update the information on our file and must if requested take reasonable steps to advise a third party to whom we have provided information that it has been updated.

REVISION HISTORY

Version	Approval date	Change
13	18 February 2025	Reviewed, minor changes made
12	30 November 2023	Reviewed, additional information around staff welfare after a data breach
11	20 March 2023	Reviewed, Minor changes made
10	29 September 2021	Minor change
9	7 December 2020	Minor updates to reflect ISMS
8	27 April 2020	Minor changes to incorporate internal audit observations
7	14 October 2019	Insert hyperlinks to the OAIC web site
6	6 December 2018	Notifiable Data Breach amendment
5	21 November 2016	Added to policy – receiving a complaint, reporting a breach and request for personal information
4	30 May 2016	Reviewed, minor amendments
3	10 March 2014	Updated in relation to the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cwth),
2	31 May 2012	Reviewed and approved with minor changes
1	1 July 2011	Company name change