# POL Privacy Policy

## Purpose

The purpose of this privacy policy is to:

- Outline how the PHN ("**the Company**") complies with the Australian Privacy Principles and relevant legislation dealing with privacy in Australia;
- Describe the personal information handling practices of the Company and enhance the transparency of its operations;
- Give staff a more complete understanding of the range of personal information that the PHN holds, and the way that information is managed; and
- Provide details of how individuals can complain or report a breach of our responsibilities in regard to privacy, and how the PHN will handle such complaints.

## Scope

This policy applies to all employees, independent contractors, consultants, and other workers engaged by the Company and who have access to personal information in the course of performing their duties.

## Policy Statement

The Company is required to collect, hold, use and/or disclose personal information relating to individuals (including, but not limited to its customers, contractors, suppliers, commissioned service providers and employees) in the performance of its business activities.

The information collected by the Company will potentially be accessible to identified individuals employed or engaged by the Company who may be required to use the information in the course of their duties.

This document sets out the Company's policy in relation to the protection of personal information, as defined, under the *Privacy Act 1988* (Cth) the ("**Act**"), which includes the *Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)* and the Australian Privacy Principles ("**APP**"). The APPs regulate the handling of personal information.

The obligations imposed on the Company under this policy are also imposed on any individual employed or engaged by the Company ("**employees"**).

This policy outlines the Company's requirements and expectations in relation to the handling of personal information.

This policy does not extend to personal information held as part of the Companys employee records.

**What is personal information?**

Personal information means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

**What is not personal information?**

This policy does not apply to the collection, holding, use or disclosure of personal information that is an employee record as they are exempt from the APPs.

An employee record is a record of personal information relating to the employment of an employee. Examples of personal information relating to the employment of the employee include, but are not limited to, health information and information about the engagement, training, disciplining, resignation, termination, terms, and conditions of employment of the employee.

Employees (such as those engaged in a supervisory, operations or human resource capacity) will have access to employee records. Employees who have access to employee records must ensure that the information is handled confidentially and for a proper purpose only. Employee records are only permitted to be collected, used, and disclosed where the act of doing so is directly related to a current or former employment relationship.

Employees who have access to employee records and who may have a question about the use or disclosure of employee records, should contact the HR & OD Manager or Executive Manager Corporate Services or Privacy Officer.

**Kinds of information that the Company collects and holds**

The Company collects personal information that is reasonably necessary for one or more of its functions or activities or if the Company has received consent to collect the information. If the Company collects sensitive information (as defined below), the Company must also have obtained consent in addition to the collection being reasonably necessary.

The type of information that the Company collects and holds may depend on an individual's relationship with the Company, for example:

a) **Candidate**: if a person is a candidate seeking employment with the Company, the Company may collect and hold information about that candidate including the candidates name, address, email address, contact telephone number, gender, age, employment history, references, resume, medical history, emergency contact, taxation details, qualifications, and payment details.
b) **Customer**: if a person is a customer of the Company, the Company may collect and hold information including the customer's name, address, email address, contact telephone number, gender and age and other sensitive information.
c) **Supplier**: if a person or business is a supplier of the Company, the Company may collect and hold information about the supplier including the supplier's name, address, email address, contact telephone number, business records, billing information and information about goods and services supplied by the supplier.
d) **Commissioned Service Providers**: if a person or business delivers services funded by the Company, the Company may collect and hold information about the Service Provider or Service Provider's Personnel including name, address, email address, contact telephone number, business records, qualifications, and payment details**.**
e) **Referee**: if a person is a referee of a candidate being considered for employment by the Company, the Company may collect and hold information including the referee's name, contact details, current employment information and professional opinion of candidate.
f) **Sensitive information:** the Company will only collect sensitive information where an individual consents to the collection of the information and the information is reasonably necessary for one or more of the Company's functions or activities. Sensitive information includes, but is not limited to, information or an opinion about racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs, membership of a trade union, sexual preferences, criminal record, health information or genetic information.
g) **Potentially identifiable information:** subject to strict data sharing agreements, the Company may collect deidentified information of a clinical nature from health care providers such as General Practices or commissioned mental health service providers. Although deidentified, it may be possible in some instances to filter clinical information which may potentially identify a patient or client of a service or provider. Strict data governance policies and procedures apply to this information.

**How the Company collects and holds personal information**

The Company (and the employees acting on the Company's behalf) must collect personal information only by lawful and fair means.

The Company may collect personal information in a number of ways, including without limitation:

i. through application forms (e.g., job applications, program applications);
ii. by email or other written mechanisms;
iii. over a telephone call;
iv. in person;
v. through transactions;
vi. through the Company website;
vii. through lawful surveillance means such as a surveillance camera;
viii. by technology that is used to support communications between individuals or organisations and the Company (Folio, PATCAT, surveys and PROMS/PREMS);
ix. through publicly available information sources (which may include telephone directories, the internet, and social media sites); and
x. direct marketing database providers.

When the Company collects personal information about an individual through publicly available information sources, it will manage such information in accordance with the APPs.

At or before the time or, if it is not reasonably practicable, as soon as practicable after, the Company collects personal information, the Company must take such steps as are reasonable in the circumstances to either notify the individual or otherwise ensure that the individual is made aware of the following:

i. the identity and contact details of the Company;
ii. that the Company has collected personal information from someone other than the individual or if the individual is unaware that such information has been collected;
iii. that collection of personal information is required by Australian law, if it is;
iv. the purpose for which the Company collects the personal information;
v. the consequences if the Company does not collect some or all of the personal information;
vi. any other third party to which the Company may disclose the personal information collected by the Company;
vii. the Company's privacy policy contains information about how an individual may access and seek correction of personal information held by the Company and how an individual may complain about a breach of the APPs; and
viii. whether the Company is likely to disclose personal information to overseas recipients, and the countries in which those recipients are likely to be located.

**Unsolicited personal information** is personal information that the Company receives which it did not solicit. Unless the Company determines that it could have collected the personal information in line with the APPs or the information is contained within a Commonwealth record, it must destroy the information to ensure it is de-identified unless the Company determines that it is acceptable for the Company to have collected the personal information.

**Use and Disclosure of Personal Information**

The main purposes for which the Company may use and/or disclose personal information may include but are not limited to:

i. recruitment functions;
ii. customer service management;
iii. training and events;
iv. meet reporting deliverables to the Department of Health/ Board/Other funding bodies or Stakeholders e.g., Workplace Gender Equity Reporting
v. surveys and general research; and
vi. business relationship management.

The Company may also collect, hold, use and/or disclose personal information if an individual consents or if required or authorised under law.

Direct marketing:

i. the Company may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing (for example, advising community or staff about services being offered by the Company);
ii. the Company may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose; and
iii. an individual can opt out of receiving direct marketing communications from the Company by contacting the Privacy Officer in writing or if permissible accessing the Company's website and unsubscribing appropriately.

**Disclosure of Personal Information**

The Company may disclose personal information for any of the purposes for which it is was collected, as indicated under clause 6 of this policy, or where it is under a legal duty to do so.

Disclosure will usually be internally and to related entities or to third parties such as contracted service suppliers, contract service providers, the Department of Health and or the Board of Directors.

If an employee discloses personal information to a third party in accordance with this policy, the employee must take steps as are reasonable in the circumstances to ensure that the third party does not breach the APPs in relation to the information.

**Access to personal information**

If the Company holds personal information about an individual, the individual may request access to that information by putting the request in writing and sending it to the Privacy Officer. The Company will respond to any request within a reasonable period, and a charge may apply for giving access to the personal information where the Company incurs any unreasonable costs in providing the personal information.

There are certain circumstances in which the Company may refuse to grant an individual access to personal information. In such situations the Company will provide the individual with written notice that sets out:

i. the reasons for the refusal; and
ii. the mechanisms available to you to make a complaint.

If you receive such a request, please contact the HR & OD Manager, Executive Manager Corporate Services, or the Privacy Officer.

**Correction of personal information**

If the Company holds personal information that is inaccurate, out-of-date, incomplete, irrelevant, or misleading, it must take steps as are reasonable to correct the information.

If the Company holds personal information and an individual makes a request in writing addressed to the Privacy Officer to correct the information, the Company must take steps as are reasonable to correct the information and the Company will respond to any request within a reasonable period.

There are certain circumstances in which the Company may refuse to correct the personal information. In such situations the Company will give the individual written notice that sets out:

i. the reasons for the refusal; and
ii. the mechanisms available to the individual to make a complaint.

If the Company corrects personal information that it has previously supplied to a third party and an individual requests the Company to notify the third party of the correction, the Company will take such steps as are reasonable to give that notification unless impracticable or unlawful to do so.

If you receive such a request, please contact the HR & OD Manager, Executive Manager Corporate Services, or the Privacy Officer.

**Integrity and security of personal information**

The Company will take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that it collects is accurate, up-to-date, and complete.

Employees must take steps as are reasonable in the circumstances to protect the personal information from misuse, interference, loss and from unauthorised access, modification, or disclosure.

If the Company holds personal information and it no longer needs the information for any purpose for which the information may be used or disclosed and the information is not contained in any Commonwealth record and the Company is not required by law to retain the information, it will take such steps as are reasonable in the circumstances to destroy the information or to ensure it is de-identified.

If you are unsure whether to retain personal information, please contact please contact the HR & OD Manager, Executive Manager Corporate Services, or the Privacy Officer.

**Data Breaches and Notifiable Data Breaches**

A "**Data Breach**" occurs where personal information held by the Company is accessed by, or is disclosed to, an unauthorised person, or is lost. An example of a Data Breach may include:

i. Lost or stolen laptops or tablets;
ii. Lost or stolen mobile phone devices;
iii. Lost or stolen USB data storage devices;
iv. Lost or stolen paper records or documents containing personal information relating to the Employer's customers or employees;
v. Employees mistakenly providing personal information to the wrong recipient (i.e., payroll details to wrong address);
vi. Unauthorised access to personal information by an employee;
vii. Employees providing confidential information to the Employer's competitors;
viii. Credit card information lost from insecure files or stolen from garbage bins;
ix. Where a database has been 'hacked' to illegally obtain personal information;
x. Any incident or suspected incident where there is a risk that personal information may be misused or obtained without authority; and
xi. If you are aware of or reasonably suspect a Data Breach, you must report the actual or suspected Data Breach to General Manager as soon as reasonably practicable and not later than 24 hours after becoming aware of the actual or suspected Data Breach.

A "**Notifiable Data Breach"** occurs where there is an actual Data Breach, and:

i. a reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to the relevant individual (including harm to their physical or mental well-being, financial loss, or damage to their reputation); or
ii. in the case of loss (i.e., leaving an unsecure laptop containing personal information on a bus), unauthorised access or disclosure of personal information is likely to occur as a result of the Data Breach, and a reasonable person would conclude that the unauthorised access or disclosure would likely result in serious harm to the relevant individual (including harm to their physical or mental well-being, financial loss, or damage to their reputation).

A Notifiable Data Breach does not include a Data Breach where the Company has been successful in preventing the likely risk of serious harm by taking remedial action.

<u>Assessment</u>

If the Company is aware of any actual or suspected Data Breach, it will conduct a reasonable and expeditious assessment to determine if there are reasonable grounds to believe that the Data Breach is a Notifiable Data Breach or not.

Notification

Subject to any restriction under the Act, in the event that the Company is aware of a Notifiable Data Breach, the Company will, as soon as practicable, prepare a statement outlining details of the breach and notify:

i. the individual whose personal information was part of the Data Breach; and
ii. the Office of the Australian Information Commissioner.

**Anonymity and Pseudonymity**

Individuals have the option of not identifying them self, or using a pseudonym, when dealing with the Company in relation to a particular matter. This does not apply:

i. where the Company is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or
ii. where it is impracticable for the Company to deal with individuals who have not identified themselves or who have used a pseudonym.

However, in some cases if an individual does not provide the Company with the personal information when requested, the Company may not be able to respond to the request or provide you with the goods or services that you are requesting.

**Complaints**

Individuals have a right to complain about the Company's handling of personal information if the individual believes the Company has breached the APPs.

If an employee becomes aware of an individual wanting to make such a complaint to the Company, the employee should direct the individual to first contact Privacy Officer or Executive Manager in writing. Complaints will be dealt with in accordance with the Company's complaints Management Policy or Provider Critical Incident or Complaint Reporting policy and the Company will provide a response within a reasonable period.

Individuals who are dissatisfied with the Company's response to a complaint, may refer the complaint to the Office of the Australian Information Commissioner.

**Breach of this policy**

An employee directed by the Company to do an act under this policy, and which relates to personal information, must ensure that in doing the act they comply with the obligations imposed on the Company. An employee directed by the Company who fails to do an act in accordance with this policy will be deemed to have breached this policy and will be subject to formal counselling and disciplinary action, up to and including possible termination of the employee's employment.

We may amend this policy from time to time in order to ensure that it remains accurate in view of any alterations to our information handling practices due to new technologies and changed business practices. Any updated policy and changes to legislation will be published on the PHN website

## Roles and Responsibilities

The PHN Privacy Officer is:
The HR & OD Manager
Kelly Pumpa
Kpumpa@thephn.com.au

The IT Privacy Officer is;

IMIT Manager
Jason Rumianek
IT@thephn.com.au

The Privacy Officers are responsible for the Privacy Management Framework which incorporates the Privacy Compliance Framework and the Privacy Audits as well as the monitoring of changes to legislation and guidelines. Specific roles in regard to the protection of personal information are outlined in the Privacy Compliance Framework.

## Supporting Procedures

**Privacy Compliance Framework**

To minimise and manage privacy risks, the Company implements practices, procedures, and systems to ensure compliance as required by Australian Privacy Principle (APP) 1 – Open and transparent management of personal information. The Company Privacy Compliance Framework is available in the Digital Workspace. The Privacy Officer undertakes the activities required in the framework as well as regular reviews as outlined.

The Company conducts regular reviews of systems, processes, and staff awareness of obligations in relation to privacy.

Results of an annual privacy audit conducted in each area of the business are reported to the Executive team together with recommendations about any changes required to achieve compliance with legislated requirements and to improve standards.

The Privacy Officer is responsible for ensuring that audits are undertaken in accordance with this policy and that results are documented and reported.

Portfolio Executive Managers (or their delegated authority) are required to conduct annual privacy discussions with staff, generally during a team meeting. To help facilitate the discussion, the Privacy Self-Assessment Survey is completed and returned to the Privacy Officer. On completion of each audit, the Privacy Officer compiles a report to the Executive making recommendations about any identified opportunities to improve compliance.

## References/Related Documents

- Privacy Act 1988 (Cwlth)
- Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cwlth)
- Health Records and Information Privacy Act 2002 (NSW)
- Privacy Audit Questionnaire
- Privacy Compliance Framework
- The PHN Privacy Management Framework
- Complaints Management Policy
- Provider Critical Incident or Complaint Reporting

## Document Control

| | |
|---|---|
| **Policy Sponsor:** | Corporate Services Executive Manager |
| **Distribution:** | All PHN Staff |
| **Policy Approved by:** | Corporate Services Executive Manager |
| **Review Frequency:** | Biennial |
| **Date Approved:** | 11 September 2021 |

| | |
|---|---|
| **Review Date:** | 11 September 2023 |

## Revision History

| Version | Status * | Author | Date | Reason for amendment |
|---|---|---|---|---|
| V0.0 | Draft | Maureen Beckett | 2015 | Draft |
| V1.0 | Approved | Maureen Beckett | 23/09/2025 | Approved by CEO |
| | Amended | Maureen Beckett | 5/4/2016 | Amended Newcastle office address |
| | Reviewed | Maureen Beckett | 18/09/2019 | Reviewed and update |
| V0.2 | Draft | Kirby Wall | 14/07/2021 | Reviewed and rewritten |
| | Reviewed and approved | Kelly Pumpa, Kirby Wall, David Martens, Jason Rumianek, Jacqui Kelleher, Lorin Livingstone | 11/9/2021 | Reviewed and updated |

**Status: Draft/ Approved/ Amended/ Rescinded*