

Privacy Statement

The role of the Network in working with General Practice and their data

.....

Purpose

This privacy statement is based on the privacy policy of the Network. It specifically addresses privacy related to patient data collected at a General Practice for the purpose of the Network's programs and services.

Copies of the full privacy policy can be obtained by contacting the Privacy Officer of the PGPN (ph: 9708 8019 email: contact@pgpn.org.au).

General Practice data – practice support by the Network

When a member of the Network undertakes some support for a practice, be it with an individual General Practitioner, Practice Nurse or other Practice staff member, it must be clearly understood that the patient data is data owned by the practice.

With regard to the individual patient, the policy of consent relating to the individual patient rests between the patient and the General Practice. When the patient provides the data to the practice, there is a clear understanding that the GP and his/her support team will use the data for the assistance of the patient. Most practices have a consent process established as part of their AGPAL accreditation process.

The Network should clarify with practices that they have established such a patient consent process.

The role of the Network staff member who works with the practice is similar to role of other external people who work with the practice, such as IT system support staff that a practice may employ, or the accountant of the practice, who has potential access to all the billing details of each patient as part of the ongoing financial management of the practice.

Accordingly, the Network use of the patient data relates to work that we undertake to assist that practice. Sometimes, the data may be taken off site to enable more work to be undertaken. The Network has in place systems to protect the confidentiality of the data.

Approval by the Practice

Where the Network seeks to use the aggregated data from a practice to help build its knowledge of the collective profile of practices in the Peninsula Network area, approval should be sought from the General Practice (preferably in writing).

Research

The Network may seek to use de-identified aggregated data for research purposes.

Reference to the protocols used by the Australian Bureau of Statistics with their census data provides a relevant benchmark.¹

The Bureau randomises person data when there are too few persons in a collection district, which comprises of 200 –250 households. The Bureau randomises the data up to three collection districts.

The PGPN currently only uses data aggregated to the postcode level, which is many times larger than an individual collection district.

Data used by the Network can also be coded on a range of scales when mapping. For example, the distribution may be presented as percentiles (1%–5%, 5%-10% and so on). Postcodes are grouped, so that it would be rare to show one with only 1 entry. In this sense we have randomised the data so that it would be very difficult to identify an individual patient.

Permission should also be sought from the participating practices when publishing results. The participating practices will also often be invited to form part of the authors for such research.

Kath Ferry
Chief Executive Officer

¹ Australian Bureau of Statistics. *2001 Census of Population and Housing fact sheet: confidentiality of census output.*

Privacy Policy

Purpose

This policy outlines the Peninsula GP Network privacy policy for the handling of personal information of the Network's programs and services.

National Privacy Principles (NPC)

This policy draws from the National Privacy Principles (NPPs). The ten NPPs form the core of the private sector provisions of the Privacy Act and set the minimum standards for privacy that organisations must meet.²

Principle	Description
1 Collection Collection of personal information must be fair, lawful and not intrusive. A person must be told the organisation's name, the purpose of collection, that the person can get access to their personal information and what happens if the person does not give the information.	<ol style="list-style-type: none"> 1. This Network will only collect personal information necessary to undertake our programs, activities or functions. <ol style="list-style-type: none"> 1.1. Personal information about an individual will only be collected by lawful and fair means and directly from the individual wherever possible. 1.2. The name and telephone number of the appropriate member of staff will be provided to every individual who provides personal information. 1.3. We will ensure that each individual providing personal information is informed about and understands the purpose of collecting the information, to whom or under what circumstances their personal information may be disclosed to another party, and how they can access the information held about them by the Network. 1.4. We will ensure that individuals providing personal information understand the

² Office of the Federal Privacy Commissioner (2001). *Health Information and the Privacy Act 1988: a short guide for the private health sector*. Office of the Federal Privacy Commissioner: Canberra. www.privacy.gov.au.

Principle	Description
<p>2 Use & Disclosure</p> <p>An organisation should only use or disclose information for the purpose it was collected unless the person has consented, or the secondary purpose is related to the primary purpose and a person would reasonably expect such use or disclosure, or the use is for direct marketing in specified circumstances, or in circumstances related to public interest such as law enforcement and public or individual health and safety.</p>	<p>consequences, if any, of providing incomplete or inaccurate information.</p> <p>2. This Network will ensure that personal information will only be used for the purpose it was collected, or that would reasonably be expected by the individual providing the information.</p> <p>2.1. If the identified information is to be used for a secondary or unrelated purpose, such as data analysis or research, we will obtain informed consent from the individual.</p> <p>2.1.1. Individuals will be given the opportunity to refuse such use or disclosure.</p> <p>2.1.2. If an individual is physically or legally incapable of providing consent, a responsible person (as described under the Act) may do so.</p> <p>2.2. We will only disclose personal information without consent where such disclosure is required by law, or for law enforcement, or in the interests of the individual's or the public's health and safety.</p> <p>2.2.1. We will keep records of any such use and disclosure.</p> <p>2.2.2. Information may be disclosed to a responsible person (as described under the Act).</p>
<p>3 Data Quality</p> <p>An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.</p>	<p>3. This Network will take reasonable steps to ensure that personal information kept, used or disclosed by the Network is accurate, complete, and as up to date as practicable.</p>
<p>4 Data Security</p> <p>An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access modification or disclosure.</p>	<p>4. All personal information held by this Network will be:</p> <ul style="list-style-type: none"> • if in paper form, received and stored in a secure, lockable location; • if in electronic form, password and firewall protected; • accessible by staff only on a "need to know" basis; • not taken from the Network offices unless authorised and for a specified purpose. <p>4.1. We will destroy or permanently de-identify personal information that is no longer required by the Network.</p>

Principle	Description
<p>5 Openness An organisation must have a policy document outlining its information handling practices and make this available to anyone who asks.</p>	<p>5. This policy will be made available to any person requesting access to it.</p> <p>5.1. A general statement describing our approach to privacy will be on public display at the Network.</p>
<p>6 Access & Correction Generally speaking, an organisation must give an individual access to personal information it holds about that individual on request.</p>	<p>6. Under normal circumstances this Network will provide an individual with access to their personal information within 30 days of receiving a request for access.</p> <p>6.1. There will be no fee associated with lodging a request for access, however, a small but reasonable administration fee may be charged.</p> <p>6.2. Provision of access to a person's personal information will be undertaken in a way that is appropriate to the person's particular circumstances, eg use of interpreters etc.</p> <p>6.3. If an individual believes that information held by the Network is inaccurate or incomplete, the Network will take steps to amend or correct the information.</p> <p>6.4. The Network may refuse access if it reasonably believes that:</p> <p>6.4.1. A person's health, safety or wellbeing may be compromised by releasing the information; or</p> <p>6.4.2. Providing access would be unlawful or would prejudice a legal investigation.</p> <p>6.5. Under circumstances other than 6.4.1 and 6.4.2 where information is withheld, the Network will ensure that its practices are consistent with the provisions of NPP 6.</p> <p>6.6. If information is withheld under 6.4, the Network will provide an explanation to the individual as to the reasons why this was the case.</p>
<p>7 Identifiers Generally speaking an organisation must not adopt, use or disclose, an identifier that has been assigned by a Commonwealth government</p>	<p>7. Except where circumstances allow (NPP7.2), this Network will not use Medicare or Veterans Affairs numbers or other identifiers assigned by a Commonwealth or State/Territory agency to identify personal information.</p>

Principle	Description
'agency'.	
<p>8 Anonymity Organisations must give people the option to interact anonymously whenever it is lawful and practicable to do so.</p>	<p>8. Where it is lawful and practicable to do so, the Network will allow individuals to provide information anonymously.</p> <p>8.1. An individual who chooses to access the services of the Network anonymously will be advised of any potential consequences resulting from their decision. Eg where the lack of a contact name or address may jeopardise care in an emergency situation.</p> <p>8.2. We will not automatically preclude an individual from participating in the activities of the Network because they request anonymity.</p>
<p>9 Transborder Data Flows An organisation can only transfer personal information to a recipient in a foreign country in circumstances where the information will have appropriate protection.</p>	<p>9. This Network will only transfer personal information about an individual to someone who is in a foreign country if:</p> <ul style="list-style-type: none"> • the individual consents to the transfer; or • the recipient is bound by legislation that is substantially similar to the NPPs; or • we are reasonably sure that the information will not be held, used or disclosed inconsistently with the NPPs.
<p>10 Sensitive Information An organisation must not collect sensitive information unless the individual has consented, it is required by law – or in other special specified circumstances, for example, relating to health services provision and individual or public health or safety.</p>	<p>10. This Network will only collect sensitive information (as defined under the Act) other than health information about an individual if:</p> <ul style="list-style-type: none"> • the individual consents; or • the collection is required by law; or • such collection is consistent with the provisions of NPP 10