



# North East Valley Division of General Practice

Level 1 North Wing, Repatriation Hospital  
Heidelberg West VIC 3081

Locked Bag 1, Heidelberg West VIC 3081

Telephone: (03) 9496 4333 Facsimile: (03) 9496 4349

Email: [nevdgp@nevdgp.org.au](mailto:nevdgp@nevdgp.org.au) Website: [www.nevdgp.org.au](http://www.nevdgp.org.au)

## PRIVACY POLICY

DATE ADOPTED : AUGUST 2005

DATE REVIEWED: AUGUST 2007

### Protecting the Privacy of your Personal Information

In complying with the Privacy Amendment (Private Sector) Act 2000, North East Valley Division of General Practice has developed a Privacy Policy that governs its handling of 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 a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.*

(p57 Guidelines on Privacy in the Private Health Sector, Office of the Federal Privacy Commissioner - October 2001)

Our Privacy Policy governs:

- what personal information is being collected;
- who is collecting personal information;
- how personal information is used;
- to whom and under what circumstances personal information is disclosed; and
- how personal information is stored.

In most circumstances, NEVDGP will:

- only collect personal information about you with your consent (unless legally required or authorised to do otherwise);
- collect your personal information directly from you (where possible and practicable);
- only collect personal information about you that is necessary and relevant to the purpose for which it is collected;
- use staff to collect your information who are appropriately trained and have a specific role in the purpose for which your personal information is being collected;
- only use your 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);
- provide you with access to your personal information (unless legally required or authorised to do otherwise). A small but reasonable administration fee may be levied to provide such access;
- only disclose your personal information to a third party with your consent, or where you expect such disclosure, or where we are legally required or authorised to do so;
- take reasonable steps to keep your personal information complete, current and accurate.

<p><b>1 Collection</b></p> <p>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.</p>	<ol style="list-style-type: none"> <li>1. This Division will only collect personal information necessary to undertake our programs, activities or functions. <ol style="list-style-type: none"> <li>1.1. Personal information about an individual will only be collected by lawful and fair means and directly from the individual wherever possible.</li> <li>1.2. The name and telephone number of the appropriate member of staff will be provided to every individual who provides personal information.</li> <li>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 Division.</li> <li>1.4. We will ensure that individuals providing personal information understand the consequences, if any, of providing incomplete or inaccurate information.</li> </ol> </li> </ol>
<p><b>2 Use &amp; Disclosure</b></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>	<ol style="list-style-type: none"> <li>2. This Division 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. <ol style="list-style-type: none"> <li>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. <ol style="list-style-type: none"> <li>2.1.1. Individuals will be given the opportunity to refuse such use or disclosure.</li> <li>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.</li> </ol> </li> <li>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. <ol style="list-style-type: none"> <li>2.2.1. We will keep records of any such use and disclosure.</li> <li>2.2.2. Information may be disclosed to a responsible person (as described under the Act).</li> </ol> </li> </ol> </li> </ol>
<p><b>3 Data Quality</b></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>	<ol style="list-style-type: none"> <li>3. This Division will take reasonable steps to ensure that personal information kept, used or disclosed by the Division is accurate, complete, and as up to date as practicable.</li> </ol>

<p><b>4 Data Security</b> 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 Division will be:</p> <ul style="list-style-type: none"> <li>• if in paper form, received and stored in a secure, lockable location;</li> <li>• if in electronic form, password and firewall protected;</li> <li>• accessible by staff only on a “need to know” basis;</li> <li>• not taken from the Division offices unless authorised and for a specified purpose.</li> </ul> <p>4.1. We will destroy or permanently de-identify personal information that is no longer required by the Division.</p>
<p><b>5 Openness</b> 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 Division.</p>
<p><b>6 Access &amp; Correction</b> 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 Division 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 Division is inaccurate or incomplete, the Division will take steps to amend or correct the information.</p> <p>6.4. The Division 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 6.3.1 and 6.3.2 where information is withheld, the Division will ensure that its practices are consistent with the provisions of NPP 6.</p> <p>6.6. If information is withheld under 6.1, the Division will provide an explanation to the individual as to the reasons why this was the case.</p>

<p><b>7 Identifiers</b></p> <p>Generally speaking an organisation must not adopt, use or disclose, an identifier that has been assigned by a Commonwealth government 'agency'.</p>	<p>7. Except where circumstances allow (NPP7.2), this Division will not use Medicare or Veterans Affairs numbers or other identifiers assigned by a Commonwealth or State/Territory agency to identify personal information.</p>
<p><b>8 Anonymity</b></p> <p>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 Division will allow individuals to provide information anonymously.</p> <p>8.1. An individual who chooses to access the services of the Division 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 Division because they request anonymity.</p>
<p><b>9 Transborder Data Flows</b></p> <p>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 Division will only transfer personal information about an individual to someone who is in a foreign country if:</p> <ul style="list-style-type: none"> <li>• the individual consents to the transfer; or</li> <li>• the recipient is bound by legislation that is substantially similar to the NPPs; or</li> <li>• we are reasonably sure that the information will not be held, used or disclosed inconsistently with the NPPs.</li> </ul>
<p><b>10 Sensitive Information</b></p> <p>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 Division 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"> <li>• the individual consents; or</li> <li>• the collection is required by law; or</li> <li>• such collection is consistent with the provisions of NPP 10</li> </ul>