Privacy and personal information

The Privacy and Personal Information Protection Act, 1998 (PPIPA) provides protection for personal information and the privacy of individuals in general. To achieve this PPIPA introduces a set of privacy principles that regulate the way Council deals with personal information.

Narrandera Shire Council is committed to protecting the privacy of our customers, business contacts, Councillors, employees, contractors and volunteers. The Privacy Management Plan details how Narrandera Shire Council manages the personal and health information it collects, stores, accesses, uses and discloses in the course of its business activities.

Privacy Management Plan

The Privacy and Personal Information Protection Act 1998 [PPIPA] requires all public sector agencies to prepare, implement and review their Privacy Management Plan at least every three years. This policy outlines how Narrandera Shire Council complies with the legislative requirements of the PPIPA, the Health Records and Information Privacy Act 2002 [HRIPA] and the Privacy Code of Practice for Local Government [Code].

It is designed to inform the community and educate staff on access to personal information and to introduce Council policies and procedures to maximise compliance with the PPIPA and the HRIPA.

Privacy code of practice for Local Government

A Privacy Code of Practice (for Local Government) was approved by the Attorney General and is binding on all local government authorities. The Code modifies the privacy principles and the public register provisions of the Privacy Act and enables Councils to fulfil their statutory duties whilst still complying with the Act

What is personal information?

Personal information is defined as:
"information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. This information can be on a database and does not necessarily have to be recorded in a material form".

What is not personal information?

Personal information does not include information about an individual that is contained in a publicly available publication. Personal information, once it is contained in a publicly available publication, ceases to be covered by the PPIPA.

Where the Council is requested to provide access or make a disclosure and that information has already been published, then the Council will rely on the provisions of the relevant Act that authorises Council to hold that information and not the PPIPA (for example, a formal or informal request under the Government Personal information does not include information about an individual that is contained in a publicly available publication. Personal information, once it is contained in a publicly available publication, ceases to be covered by the PPIPA.

How is personal information protected?

Information is protected by a number of information protection principles contained within the Act. In general terms, the principles apply to the way material is collected, stored, used and disclosed. A summary of the information protection principles appears at the end of this page. It should be noted that the privacy legislation relates to personal information only.

What is a public register?

A public register is defined as "a register of personal information that is required by law to be, or is made, publicly available or open to public inspection (whether or not on payment of a fee)".

Council holds public registers under the LGA, including:

- Land Register
- Records of Approvals
- Register of Disclosures of Interests

Council, as a local authority, may hold other public registers, to which PPIPA applies.

Council holds public registers under the Environmental Planning and Assessment Act 1979 [EPA]:

- Register of consents and certificates
- Record of building certificates

Council holds a public register under the Protection of the Environment Operations Act 1997 [POEO]:

- Public register of licences

Council holds a public register under the Impounding Act 1993 [IA]:

- Record of impounding

The register required to be kept under the Companion Animals Act, 1998 is not considered to be a public register in terms of the PPIP Act.

Request for information held on a public register?

Requests for access, copying or the sale of the whole or a substantial part of a public register held by Council will not always fit within the purpose of a particular register. Council will be guided by the Code in this respect and will make an assessment as to the minimum amount of personal information that is required to be disclosed.

Where council officers have doubt as to the intended use of the information, an applicant may be requested to provide a statutory declaration so that Council may satisfy itself as to the intended use of the information. Council will make its assessment as to the minimum amount of personal information that is required to be disclosed with regard to any request.

What is a legitimate purpose?

According to the Information & Privacy Commission NSW most public concern about privacy breaches from councils relate to personal information disclosed from the rate record.

The primary purpose of rate record is to record the value of a parcel of land and record rate liability in respect of that land. The secondary purpose includes recording the owner or lessee of each parcel of land. Due to the emphasis on local government processes and information being open and accountable, it is considered that a secondary purpose for which all public registers are held includes the provision of access to members of the public. Of course only the minimum amount of personal information should be disclosed in regard to any request.

Use by Council

Legitimate Council use would include:

- levying of rates on a property
- taking out easements over properties
- bushfire hazard & noxious weed control
- law enforcement
- notification of development proposals
- administrative purposes

Use by government agencies

Applications for personal information from a register (bulk listings etc) should be in writing and proposed use should be clearly stated. The use should always relate to activities associated with the functions of that agency. Other government agencies such as Centrelink and Veterans Affairs will be provided with information where there is a legal requirement to do so.

Business use

One of the main reasons for including public register provisions in privacy legislation was to provide a means of addressing widespread public concerns over the commercial sale of council information. It was generally felt that the information was being used for a reason that had no clear relationship to the reasons for which it was collected. The use of information for marketing purposes therefore needs to be distinguished from legitimate professional use by valuers and real estate agents.

With regard to the sale of bulk data (rate record and building/development statistics), Council has taken steps to remove all personal information (names & mailing addresses) from lists and subscribers have been advised accordingly. Lists containing property information only, will continue to be made available for inspection or purchase.

Land transfer notices have traditionally been made available for the inspection of valuers. It is recognised that the names of vendors and purchasers are required in order that valuers can establish whether the price reflects a sale or not. Whilst councils are not the only source of this information this is considered to be a legitimate use and Council will therefore allow this access to continue.

Public use

Legitimate uses would include those relating to;

- possible sale of a property (prospective purchasers)
- dividing fences
- conveyancing matters
- proposals for use of land (agistment, parking)
- notifications of backyard burning
- contact with property owners re complaints (drainage, trees, noise etc)
- matters involving the safety of a person
- matters where it is considered that the person would want to be contacted
- A person wishing to access their own details from a public register need only to prove their identity to Council.

Inappropriate use

Whilst inappropriate uses are more difficult to define, examples could include;

- where the information was to be used for marketing purposes
- where it is reasonable to assume that the applicant is contemplating a violent act against the person who is the subject of the enquiry
- where the information is to be used for private debt recovery purposes
- where the person named on the register is unlikely to agree to the release of the information for the reason given (apart from those legitimate uses mentioned above)

Can a person apply to have their details removed from a public register?

The Act gives people a right to have their personal details hidden or removed from a public register where they can show that the safety or well-being of any person might be affected if the information was to remain on the record. Council must suppress the information unless it is satisfied that the public interest in maintaining public access to the information outweighs any individual interest.

An application for suppression should be made in writing and addressed to the Chief Executive Officer. It must contain sufficient detail to allow for the proper assessment of the application and supporting documentation may be required.

Can a person apply to have their details removed from a public register?

The Act gives people a right to have their personal details hidden or removed from a public register where they can show that the safety or well-being of any person might be affected if the information was to remain on the record. Council must suppress the information unless it is satisfied that the public interest in maintaining public access to the information outweighs any individual interest.

An application for suppression should be made in writing and addressed to the Chief Executive Officer. It must contain sufficient detail to allow for the proper assessment of the application and supporting documentation may be required.

What can an individual do if personal information is collected or used wrongly?

A number of legal remedies are available to people who feel they have had their privacy breached. The aggrieved person may lodge a complaint with the Privacy Commissioner or apply to Council for a review of the conduct which is the subject of the complaint.

There are five possible things an agency can do about a complaint. It can:

- apologise;
- offer a remedy such as compensation;
- promise that the behaviour will not occur again;
- change its operations to make sure that the behaviour will not occur again;
- or do nothing.

If the complainant is not satisfied with the Council's findings or what Council proposes to do, they can appeal to the Administrative Decisions Tribunal. One of the more significant orders the Administrative Decisions Tribunal can make is awarding damages of up to $40,000 to the person making the complaint, where that person has suffered financial loss or was physically or psychologically injured.

Offences

The Act details offences for corruptly dealing with personal information. Harsh penalties (up to a maximum of $11,000 and 2 years in prison) can be given if public sector officials, including former public sector officials, deliberately disclose, or offer to supply personal information outside of their lawful powers. Penalties also apply to any other persons who induce or attempt to induce a public sector official to act in this way (eg bribes and other such conduct).

Information protection principles

The information protection principles are summarised as follows:-

Principle 1 - Collection of information for lawful purposes

- personal information must not be collected unless for a lawful purpose which is directly related to function or activity of the agency and collection is reasonably necessary for that purpose
- collection of personal information must not be by any unlawful means

Principle 2 - Collection of information directly from the individual

- personal information must be collected directly from the individual unless that person has authorised collection from someone else; or
- in the case of a person under 16 years of age, collection may be from a parent or guardian of the person.

Principle 3 - Requirements when collecting information

If collected from an individual reasonable steps must be taken to ensure that, before collection or soon after, the individual is aware of:

- the collection of the information
- purpose of collection
- intended recipients of the information
- whether supply of information was required by law or voluntary
- existence of rights of access to and/or correction of information
- the name & address of agency collecting and the agency that is holding the information

Principle 4 - Other requirements relating to collection of personal information

- collection must be relevant, not excessive, accurate & up to date and complete
- collection does not intrude, to an unreasonable extent, on the personal affairs of an individual

Principle 5 - Retention & security of personal information

In holding information Council must ensure that:-

- it is not kept for longer than necessary for lawful use
- it is disposed of securely and lawfully
- reasonable steps are taken to protect against loss, unauthorised access, use, modification or disclosure & all other misuse
- reasonable steps are taken to protect against misuse outside Council (consultants, contractors)

Principle 6 - Information about personal information held by Council

Council must take such steps as are reasonable to enable any person to ascertain:

- whether personal information is held by Council, generally
- whether personal information is held about that person and if so, the nature of information, purpose of use & entitlement to access

Principle 7 - Access to personal information held by Council

Council must provide access to information to an individual to whom the information relates

Principle 8 - Alteration of personal information

Personal information of the individual concerned must be amended on request so as to ensure accuracy

Principle 9 - Accuracy of information

Personal information must not be used unless, prior to use, reasonable steps have been taken to ensure its accuracy

Principle 10 - Limits of use of information

Personal information must not be used for any purpose other than the purpose for which it was collected unless:

- the individual consents to the use the other purpose relates to the original purpose for collection
- use of information would prevent or lessen a serious & imminent threat to life or health of the individual.

HEALTH PRIVACY PRINCIPLES (HPPs)

Health information includes personal information that is information or an opinion about the physical or mental health or a disability of an individual. Health information *also* includes personal information that is information or an opinion about:

- a health service provided, or to be provided, to an individual;
- an individual's express wishes about the future provision of health services to him or her;
- other personal information collected in connection with the donation of human tissue; or
- genetic information that is or could be predictive of the health of an individual or their relatives or descendants.

HPPs 1-4 concern the collection of health information, HPP 5 concerns the storage of health information, HPPs 6-9 concern the access and accuracy of health information, HPP 10 concerns the use of health information, HPP 11 concerns the disclosure of health information, HPPs 12-13 concern the identifiers and anonymity of the persons to which health information relate, HPPs 14-15 concern the transferral of health information and the linkage to health records across more than one organisation.

<u>Health Privacy Principle 1</u> - Purposes of collection of health information:

(1) An organisation must not collect health information unless:

(a) the information is collected for a lawful purpose that is directly related to a function or activity of the organisation, and
(b) the collection of the information is reasonably necessary for that purpose.

(2) An organisation must not collect health information by any unlawful means.

Health Privacy Principle 2 - **Information must be relevant, not excessive, accurate and not intrusive:**

An organisation that collects health information from an individual must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that:

(a) the information is collected is relevant to that purpose, is not excessive and is accurate, up to date and complete, and
(b) the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

Health Privacy Principle 3 - **Collection to be from the individual concerned:**

(1) An organisation must collect health information about an individual only from that individual, unless it is unreasonable or impracticable to do so.

(2) Health information is to be collected in accordance with any guidelines issued by the Privacy Commissioner for the purposes of this clause.

Health Privacy Principle 4 - **Individual to be made aware of certain matters**

(1) An organisation that collects health information about an individual from the individual must, at or before the time it collects the information (or if that is not practicable, as soon as practicable after that time), take steps that are reasonable in the circumstances to ensure that the individual is aware of the following:

(a) the identity of the organisation and how to contact it,
(b) the fact that the individual is able to request access to the information,
(c) the purposes for which the information is collected,
(d) the persons to whom (or the type of persons to whom) the organisation usually discloses information of that kind,
(e) any law that requires the particular information to be collected,
(f) the main consequences (if any) for the individual if all or part of the information is not provided.

(2) If the organisation collects health information about an individual from someone else, it must take any steps that are reasonable in the circumstances to ensure that the individual is generally aware of the matters listed in subclause (1) except to the extent that:

(a) making the individual aware of the matters would impose a serious threat to the life or health of any individual, or
(b) the collection is made in accordance with guidelines issued under subclause (3).

(3) The Privacy Commissioner may issue guidelines setting out circumstances in which an organisation is not required to comply with subclause (2).

(4) An organisation is not required to comply with a requirement of this clause if:

(a) the individual to whom the information relates has expressly consented to the organisation not complying with it or,
(b) the organisation is lawfully authorised or required not to comply with it, or
(c) non-compliance is otherwise permitted (or necessarily implied or reasonably contemplated) under any Act or any other law including the State Records Act 1998), or
(d) compliance by the organisation would, in the circumstances, prejudice the interests of the individual to whom the information relates, or
(e) the information concerned is collected for law enforcement purposes or,
(f) the organisation is an investigative agency and compliance might detrimentally affect (or prevent the proper exercise of) its complaint handling functions or any of its investigative functions.

(5) If the organisation reasonably believes that the individual is incapable of understanding the general nature of the matters listed in subclause (1), the organisation must take steps that are reasonable in the circumstances, to ensure that any authorised representative of the individual is aware of those matters.

(6) Subclause (4) (e) does not remove any protection provided by any other law in relation to the rights of accused persons or persons suspected of having committed an offence.

(7) The exemption provided by subclause (4) (f) extends to any public sector agency, or public sector official, who is investigating or otherwise handling a compliant or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

Health Privacy Principle 5 - ***Retention and Security***

(1) An organisation that holds health information must ensure that:

(a) the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and
(b) the information is disposed of securely and in accordance with any requirements for the retention and disposal of health information, and
(c) the information is protected, by taking such security safeguards as are reasonable in the circumstances against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and
(d) if it is necessary for the information to be given to a person in connection with the provision of a service to the organisation, everything reasonably within the power of an organisation is done to prevent the unauthorised use or disclosure of the information.

> **Note**. Division 2 (Retention of health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause.

(2) An organisation is not required to comply with a requirement of this clause if:

(a) the organisation is lawfully authorised or required not to comply with it, or
(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998).

(3) An investigative agency is not required to comply with subclause (1)(a).

Health Privacy Principle 6 - ***Information about health information held by organisations***

(1) An organisation that holds health information must take such steps as are, in the circumstances, reasonable, to enable any individual to ascertain:

(a) whether the organisation holds health information, and
(b) whether the organisation holds health information relating to that individual, and
(c) if the organisation holds health information relating to that individual:
(i) the nature of that information
(ii) the main purposes for which the information is used, and
(iii) that person's entitlement to request access to the information.

(2) An organisation is not required to comply with a provision of this clause if:
(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or
(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under any Act or any other law (including the State Records Act 1998).

Health Privacy Principle 7 - ***Access to health information***

(1) An organisation that holds health information must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.

> **Note.** Division 3 (Access to health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause. Access to health information held by public sector agencies may also be available under the *Government Information (Public Access) Act 2009* or the *State Records Act 1998.*

(2) An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or
(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998).

Health Privacy Principle 8 - Amendment of health information

(1) An organisation that holds health information must, at the request of the individual to whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the health information:
(a) is accurate, and
(b) having regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to day, complete and not misleading.

(2) If an organisation is not prepared to amend health information under subclause (1) in accordance with a request by the information to whom the information relates, the organisation must, if so requested by the individual concerned, take such steps as are reasonable to attach to the information, in such a manner as is capable of being read with the information, any statement provided by that individual of the amendment sought.

(3) If health information is amended in accordance with this clause, the individual to whom the information relates is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by the organisation.

> **Note.** Division 4 (Amendment of health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause.
> Amendment of health information held by public sector agencies may also be able to be sought under the Privacy and Personal Information Protection Act 1998.

(4) An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or
(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998).

Health Privacy Principle 9 - Accuracy

An organisation that holds health information must not use the information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate and up to date, complete and not misleading.

Health Privacy Principle 10

(1) An organisation that holds health information must not use the information for a purpose (a **secondary purpose**) other than the purpose (the **primary purpose**) for which it was collected unless:

(a) **Consent**

the individual to whom the information relates has consented to the use of the information for that secondary purpose, or

(b) **Direct relation** - the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to use the information for the secondary purpose or,

Note: For example, if information is collected in order to provide a health service to the individual, the use of the information to provide a further health service to the individual is a secondary purpose directly related to the primary purpose.

(c) **Serious threat to health or welfare** - the use of the information for the secondary purpose is reasonably believed by the organisation to be necessary to lessen or prevent:

(i) a serious and imminent threat to the life, health or safety of the individual or another person, or
(ii) a serious threat to public health and safety, or

(d) **Management of health services** - the use of the information for the secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services and:

(i) either:

(A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or

(B) reasonable steps are taken to de-identify the information, and

(ii) if the information is in a form that could reasonably be expected to identify individuals, the information is not published in a generally available publication, and

(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(e) **Training** - the use of the information for the secondary purpose is reasonably necessary for the training of employees of the organisation or persons working with the organisation and:

(i) either:

(A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained

and it is impracticable for the organisation to seek the consent of the individual for the use, or

(B) reasonable steps are taken to de-identify the information, and
(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and
(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(f) **Research** - the use of the information for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest and:

(i) either:

(A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or

(B) reasonable steps are taken to de-identify the information, and
(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and
(iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purpose of this paragraph, or

(g) **Find missing person** - the use of the information for the secondary purpose is by a law enforcement agency (or such other person or organisation as may be prescribed by the regulations) for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person, or

(h) **Suspected unlawful activity, unsatisfactory professional conduct or breach of discipline** - the organisation:
(i) has reasonable grounds to suspect that:

(A) unlawful activity has been or may be engaged in, or

(B) a person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under a the Health Practitioner Regulation National Law (NSW), or

(C) an employee of the organisation has or may have engaged in conduct that may be grounds for disciplinary action, and
(ii) uses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, or

(i) **Law enforcement** - the use of the information for the secondary purpose is reasonably necessary for the exercise of law enforcement functions by law enforcement agencies in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed, or

(j) **Investigative agencies** - the use of the information for the secondary purpose is reasonably necessary for the exercise of complaint handling functions or investigative functions by investigative agencies, or

(k) **Prescribed circumstances** - the use of the information for the secondary purpose is in the circumstances prescribed by the regulations for the purposes of this paragraph.

(2) An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or
(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998).

(3) The Ombudsman's Office, Health Care Complaints Commission, Anti-Discrimination Board and Community Services Commission are not required to comply with a provision of this clause in relation to their complaint handling functions and their investigative, review and reporting functions.

(4) Nothing in this clause prevents or restricts the disclosure of health information by a public sector agency:
(a) to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration, or
(b) to any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.

(5) The exemption provided by subclause (1) (j) extends to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

Health Privacy Principle 11

(1)An organisation that holds health information must not disclose the information for a purpose (a **secondary purpose**) other than the purpose (the **primary purpose**) for which it was collected unless:

(a) **Consent** - the individual to whom the information relates has consented to the disclosure of the information for that secondary purpose, or

(b) **Direct relation** - the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to disclose the information for the secondary purpose, or

> **Note:** For example, if information is collected in order to provide a health service to the individual, the disclosure of the information to provide a further health service to the individual is a secondary purpose directly related to the primary purpose.

(c) **Serious threat to health or welfare** - the disclosure of the information for the secondary purpose is reasonably believed by the organisation to be necessary to lessen or prevent:

(i) a serious and imminent threat to the life, health or safety of the individual or another person, or
(ii) a serious threat to public health or public safety, or

(d) **Management of health services** - the disclosure of the information for the secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services and:

(i) either:

(A) that purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure, or

(B) reasonable steps are taken to de-identify the information, and
(ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and
(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(e) **Training** - the disclosure of the information for the secondary purpose is reasonably necessary for the training of employees of the organisation or persons working with the organisation and:

(i) either:

(A) that purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure, or

(B) reasonable steps are taken to de-identify the information, and
(ii) if the information could reasonably be expected to identify the individual, the information is not made publicly available, and
(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(f) **Research** - the disclosure of the information for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest and:

(i) either:

(A) that purpose cannot be served by the disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be

ascertained and it is impracticable for the organisation to seek the consent of the individual for the disclosure, or

(B) reasonable steps are taken to de-identify the information, and
(ii) the disclosure will not be published in a form that identifies particular individuals or from which an individual's identity can reasonably be ascertained, and
(iii) the disclosure of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or

(g) **Compassionate reasons** - the disclosure of the information for the secondary purpose is to provide the information to an immediate family member of the individual for compassionate reasons and:

(i) the disclosure is limited to the extent reasonable for those compassionate reasons, and
(ii) the individual is incapable of giving consent to the disclosure of the information, and
(iii) the disclosure is not contrary to any wish expressed by the individual (and not withdrawn) of which the organisation was aware or could make itself aware by taking reasonable steps, and
(iv) if the immediate family member is under the age of 18 years, the organisation reasonably believes that the family member has sufficient maturity in the circumstances to receive the information, or

(h) **Finding missing person** - the disclosure of the information for the secondary purpose is to a law enforcement agency (or such other person or organisation as may be prescribed by the regulations) for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person, or

(i) **Suspected unlawful activity, unsatisfactory professional conduct or breach of discipline -** the organisation:

(i) has reasonable grounds to suspect that:

(A) unlawful activity has been or may be engaged in, or

(B) a person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under a the Health Practitioner Regulation National Law (NSW), or

(C) an employee of the organisation has or may have engaged in conduct that may be grounds for disciplinary action, and

(ii) discloses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, or

(j) **Law enforcement** - the disclosure of the information for the secondary purpose is reasonably necessary for the exercise of law enforcement functions by law enforcement agencies in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed, or

(k) **Investigative agencies** - the disclosure of the information for the secondary purpose is reasonably necessary for the exercise of complaint handling functions or investigative functions by investigative agencies, or

(l) **Prescribed circumstances** - the disclosure of the information for the secondary purpose is in the circumstances prescribed by the regulations for the purposes of this paragraph.

(2) An organisation is not required to comply with a provision of this clause if:

(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or
(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998), or
(c) the organisation is an investigative agency disclosing information to another investigative agency.

(3) The Ombudsman's Office, Health Care Complaints Commission, Anti-Discrimination Board and Community Services Commission are not required to comply with a provision of this clause in relation to their complaint handling functions and their investigative, review and reporting functions.

(4) Nothing in this clause prevents or restricts the disclosure of health information by a public sector agency:

(a) to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration, or
(b) to any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.

(5) If health information is disclosed in accordance with subclause (1), the person, body or organisation to whom it was disclosed must not use or disclose the information for a purpose other than the purpose for which the information was given to it.

(6) The exemptions provided by subclauses (1) (k) and (2) extend to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

Health Privacy Principle 12 - **Identifiers**

(1) An organisation may only assign identifiers to individuals if the assignment of identifiers is reasonably necessary to enable the organisation to carry out any of its functions efficiently.

(2) Subject to subclause (4), a private sector person may only adopt as its own identifier of an individual an identifier of an individual that has been assigned by a public sector agency (or by an agent of, or contractor to, a public sector agency acting in its capacity as agent or contractor) if:

(a) the individual has consented to the adoption of the same identifier, or

(b) the use or disclosure of the identifier is required or authorised by or under law.

(3) Subject to subclause (4), a private sector person may only use or disclose an identifier assigned to an individual by a public sector agency (or by an agent of, or contractor to, a public sector agency acting in its capacity as agent or contractor) if:

(a) the use or disclosure is required for the purpose for which it was assigned or for a secondary purpose referred to in one or more paragraphs of HPP 10 (1) (c)-(k) or 11 (1) (c)-(l), or

(b) the individual has consented to the use or disclosure, or

(c) the disclosure is to the public sector agency that assigned the identifier to enable the public sector agency to identify the individual for its own purposes.

(4) If the use or disclosure of an identifier assigned to an individual by a public sector agency is necessary for a private sector person to fulfil its obligations to, or the requirements of, the public sector agency, a private sector person may either:

(a) adopt as its own identifier of an individual an identifier of the individual that has been assigned by the public sector agency, or

(b) use or disclose an identifier of the individual that has been assigned by the public sector agency.

Health Privacy Principle 13 - **Anonymity**

Wherever it is lawful and practicable, individuals must be given the opportunity to not identify themselves when entering into transactions with or receiving health services from an organisation.

Health Privacy Principle 14 - **Transborder data flows and data flow to Commonwealth agencies.**

An organisation must not transfer health information about an individual to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless:

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the Health Privacy Principles, or

(b) the individual consents to the transfer, or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request, or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party, or

(e) all of the following apply:
(i) the transfer is for the benefit of the individual,
(ii) it is impracticable to obtain the consent of the individual to that transfer,
(iii) if it were practicable to obtain such consent, the individual would be likely to give it, or

(f) the transfer is reasonably believed by the organisation to be necessary to lessen or prevent:
(i) a serious and imminent threat to the life, health or safety of the individual or another person, or
(ii) a serious threat to public health or public safety, or

(g) the organisation has taken reasonable steps to ensure that the information that it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Health Privacy Principles, or

(h) the transfer is permitted or required by an Act (including an Act of the Commonwealth) or any other law.

Health Privacy Principle 15 - **Linkage of health records**

(1) An organisation must not:
(a) include health information about an individual in a health records linkage system unless the individual has expressly consented to the information being so included, or
(b) disclose an identifier of an individual to any person if the purpose of the disclosure is to include health information about the individual in a health records linkage system, unless the individual has expressly consented to the identifier being disclosed for that purpose.

(2) An organisation is not required to comply with a provision of this clause if:
(a) the organisation is lawfully authorised or required not to comply with the provision concerned, or
(b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998), or
(c) the inclusion of the health information about the individual in the health records information system (including an inclusion for which an identifier of the individual

is to be disclosed) is a use of the information that complies with HPP 10 (1) (f) or a disclosure of the information that complies with HPP 11 (1) (f).

(3) In this clause: **health record** means an ongoing record of health care for an individual. **health records linkage system** means a computerised system that is designed to link health records for an individual held by different organisations for the purpose of facilitating access to health records, and includes a system or class of systems prescribed by the regulations as being a health records linkage system, but does not include a system or class of systems prescribed by the regulations as not being a health records linkage system.

For Further information about Privacy please contact:

Narrandera Shire Council
141 East Street
Narrandera NSW 2700

Telephone: (02) 6959 5510

Email:council@narrandera.nsw.gov.au

Information & Privacy Commission NSW
GPO Box 7011
SYDNEY NSW 2001

Email: ipcinfo@ipc.nsw.gov.au

Freecall: 1800 472 679

Website : www.ipc.nsw.gov.au

Administrative Decisions Tribunal Level 10 John Maddison Tower 86-90 Goulburn Street SYDNEY NSW 2000

Phone: (02) 9377 5711 Fax: (02) 9377 5723