BLAND SHIRE COUNCIL
west wyalong

POLICY STATEMENT

PRIVACY MANAGEMENT PLAN

AUTHORISATION

POLICY TYPE: *(Council or Operational)*	Council
POLICY LOCATION: *(eg. Corporate, Engineering, etc.)*	Governance & Risk
RESPONSIBLE OFFICER: *(by position title)*	Director Corporate and Community Services
AUTHORISED BY: *(GM or Director Title)*	Manex
DATE ADOPTED:	20 July 2021
ADOPTED BY: *(Manex or Council)*	COUNCIL – endorsed for consultation 18 May, 2021
MINUTE NO: *(If required)*	
REVIEW DUE DATE: *(Four years unless statutorily required sooner)*	May 2025
REVISION NUMBER:	1

DOCUMENT HISTORY

VERSION NO.	DATE	DESCRIPTION OF AMENDMENTS *Include names of former policies that this policy will replace if applicable*	AMENDED BY *(Where required)*

REVIEW OF THIS POLICY

This Policy will be reviewed within four (4) years from the date of adoption or as required in the event of legislative changes. The Policy may also be changed as a result of other amendment that are to the advantage that Council and in the spirit of this Policy. Any amendment to the Policy must be by way of a Council Resolution or the approval of the General Manager.

1. Purpose:

Bland Shire Council (Council) is committed to protecting the privacy of our customers, business contacts, volunteers and our employees.

2. Scope:

Section 33 of the *NSW Privacy and Personal Information Protection Act 1998 (PPIPA)* requires all public sector agencies to prepare, implement and periodically review a Privacy Management Plan.

3. Outcomes:

This Privacy Management Plan explains how Council complies with and manages personal and health information in accordance with the PPIPA, the *Health Records and Information Privacy Act 2002 (HRIPA)* and the Privacy Code of Practice for Local Government.

What is personal information?

Personal information under section 4 of the PPIPA is defined as *information or an opinion about an individual whose identity is apparent or can reasonably be ascertained for 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 health information?

Health information under Section 6 of the HRIPA is defined as *personal information that is information or an opinion about the physical, mental health or disability of a person, express wishes about the future provision of health services, a health service provided or to be provided, or any other personal information collected to provide or in providing a health service.*

What is not personal or health 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.

Section 4a of the PPIPA also specifically excludes 'health information', as defined by Section 6 of the HRIPA, from the definition of 'personal information', but includes 'health information' in the PPIPA's consideration of public registers.

Where Council is requested to provide access or make a disclosure and that information has already been published, then Council will rely on the provisions of the relevant Act that authorises Council to hold that information and not the PPIPA (for example, Section 8 of the *Government Information (Public Access) Act 2009 (GIPA Act).*

Council considers the following to be publicly available publications:

- An advertisement containing personal information in a local, city or national newspaper;
- Personal information on the internet;
- Books or magazines that are printed and distributed broadly to the public; and
- Personal information that may be part of a public display on view to the public.

Personal information held by Council

Council holds personal information concerning Councillors, such as:

- Personal contact information;
- Complaints and disciplinary matters;
- Pecuniary interest returns; and
- Entitlements to fees, expenses and facilities.

Council holds personal information concerning its customers, ratepayers and residents, such as:

- Rates records;
- DA applications and objections; and
- Various types of health information.

Council holds personal information concerning Employees, such as:
- Recruitment material;
- Leave and payroll data;
- Personal contact information;
- Performance management information;
- Complaints and disciplinary matters;
- Pecuniary interest returns;
- Wage and salary entitlements; and
- Health information, for example medical certificates, workers compensation claims.

Caution as to unsolicited information
Where an individual, a group or committee, not established by Council, gives Council unsolicited personal or health information, then that information will still be treated in accordance with this Plan, the Codes, the HRIPA and the PPIPA for the purposes of IPPs 5-12 and HPPs 5-15 which relate to storage, access, use and disclosure of information.

Note: for the purposes of Section 10 of the HRIPA, the Council is not considered to have "collected" health information if the receipt of the information by the Council is unsolicited.

Section 4(5) of the PPIPA also provides that personal information is not "collected" by Council if it is unsolicited.

Public registers
Council is required by law to maintain a number of public registers and to make them available for public inspection

Some of these registers contain personal information as defined in the PPIPA, the HRIPA and the GIPA Act. Section 57 of the PIPPA requires Council to ensure that access to personal information in a register is consistent with the purpose for which the register exists.

In line with this requirement, Council has developed specific rules governing disclosure of personal information on registers:
- Council will not disclose personal information kept in a public register unless the information is to be used for a purpose relating to the purpose of the Register, or an Act under which the Register is kept.
- The Privacy Code of Practice allows disclosure of single items or one page in a Register without explanation. However, such a disclosure can only occur when the person seeking the information attends Council in person.
- Council requires that any person who applies for more than one record or page from a public register, does so by completing a Statutory Declaration. Any such declaration must describe the intended use of the information requested and be witnessed by a Justice of the Peace.

The list of Council registers below specifies the main purpose of each of those registers.

Council's public register list
The GIPA Act and *Government Information (Public Access) Act Regulation 2018* (GIPA Regulation) lists information available to the public free of charge within a public register. The following is a list of Council's public registers:

- *Section 53, Local Government Act, 1993 - Land Register*

The purpose of this register is to identify all land vested in Council, or under its control. It includes a consideration of public accountabi8lity as to the land held by Council.

- *Section 113, Local Government Act, 1993 - Records of Approvals*
  The primary purpose is to identify all approvals granted under the LGA.

- *Schedule 1, GIPA Regulation, 2018 – Pecuniary Interests*
  The purpose of this register is to determine whether a Councillor, a member of a council committee or a designated officer, has a pecuniary interest in any matter with which the Council is likely to be concerned. There is a corresponding public accountability purpose.

- *Section 602, Local Government Act, 1993 – Rates and Charges Records*
  The purpose of this register is to record the value of a parcel of land and record rate liability in respect of that land and the owner or lessee of each parcel of land.

The information that is held on the Rates and Charges record is:
- Property address
- Rate liability
- Property valuation
- Owner name/s

Owner contact mailing information is not considered part of the Rates and Charges record. Owner contact mailing information will only be provided to adjoining property owners.

- *Section 100, Environmental Planning and Assessment Act, 1979 – Development Consent Approvals*
  The purpose of this register is to identify applications for development consent and other approvals, confirm determinations on appeal, and identify applications for complying development certificates.

- *Section 149G, Environmental Planning and Assessment Act, 1979 – Building Certificates*
  The purpose of this register is to identify all building certificates. Register information is available for inspection free of charge. However, copies of certificates are only available with owner's consent and the payment of the prescribed fee.

- *Section 308, Protection of the Environment Operations Act, 1997 – Public register of licences held*
  The purpose of this register is to identify all licences granted under the Act.

- *Section 30 and 31, Impounding Act, 1993 – Record of Impounding*
  The purpose of this register is to record any impounding action by Council.

Secondary purpose of all public registers
Due to the general emphasis on local government processes and information being transparent and accountable, it is considered that a secondary purpose of councils holding public registers is the provision of access to the public. Therefore, disclosure of specific records from public registers would normally be considered allowable under Section 57 of the PPIPA.

However, requests for access, copying or the sale of the whole or substantial part of a public register held by Council will not necessarily fit within this purpose. Council should be guided by the Privacy Code of Practice for Local Government in this aspect. 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.

Application for access to one's own records on a public register
A person wishing to have access to a public register to confirm their own details needs only to prove their identity to Council before having access to their own personal information.

Other registers
Council may have other registers that are not considered public registers. The Information Protection Principles, the PPIPA Act, all applicable codes, and this Privacy Management Plan apply to those databases or registers.

4. Roles and Responsibilities:

Application of this plan
The PPIPA, HRIPA and this management plan apply, wherever practicable, to:

- Councillors;
- Council employees;
- Consultants and Contractors of Council;
- Council owned businesses;
- Council committees; and
- Volunteers.

Council will take reasonable steps to ensure that all such parties are made aware that they must comply with the PPIPA, the HRIPA, any other applicable Privacy Code of Practice and this plan.

Implementation of the Privacy Management Plan

Training Seminars/Induction
During induction, all employees should be made aware that the performance management system has potential to include personal information on their individual work performance or competency.

Councillors, all staff of the Council including staff of council businesses, and members of council committees should be acquainted with the general provisions of the PPIPA, the HRIPA and in particular, the 12 Information Protection Principles (IPPs), the 15 Health Privacy Principles (HPPs), the Public Register provisions, the Privacy Code of Practice for Local Government, this Plan and any other applicable Code of Practice.

Responsibilities of the Privacy Contact Officer
It is assumed that the Public Officer within Council will be assigned the role of the Privacy Contact Officer unless the General Manager has directed otherwise.

In order to ensure compliance with PPIPA and the HRIPA, the Privacy Contact Officer will review all contracts and agreements with consultants and other contractors, rates notices, application forms of whatsoever nature, and other written requests by which personal information is collected by Council, to ensure that Council is in compliance with the PPIPA.

Interim measures to ensure compliance with IPP 3 in particular, may include the creation of stamps or printed slips that contain the appropriate wording.

The Privacy Contact Officer will ensure Council in its public areas has special provisions for working with computer screens. Computer screens may require:

- Fast screen savers;
- Face the computers away from the public; or
- Only allow the record system to show one record at a time.

Council's electronic databases should also be reviewed to ensure that they contain procedures and protocols to check the accuracy and currency of personal and health information.

The Privacy Contact Officer will also provide opinions within Council as to:

(i) Whether the personal or health information is collected for a lawful purpose;
(ii) If that lawful purpose is directly related to a function of Council; and
(iii) Whether or not the collection of that personal or health information is reasonably necessary for the specified purpose.

Any further concerns of a legal nature will be referred to Council's solicitor.

Should the Council require, the Privacy Contact Officer may assign designated officers as "Privacy Resource Officers", within the larger departments of Council. In this manner the Council may ensure that the information protection principles are more broadly understood and that individual departments have a great focus on the information protection principles and are directly applied to Council's day-to-day functions.

Distribution of information to the public

Council may prepare its own literature such as pamphlets on the PPIPA, HRIPA or it may obtain and distribute copies of literature available from the Office of the Privacy Commissioner NSW.

Internal Review

Under section 53 of the PPIPA a person (the applicant) who is aggrieved by the conduct of a council is entitled to a review of that conduct. An application for internal review is to be made within **6 months** of when the person first became aware of the conduct.

The application is to be in writing and addressed to the Council's Privacy Contact Officer. The Privacy Contact Officer will appoint a Reviewing Officer to conduct the internal review. The Reviewing Officer must not be substantially involved in any matter relating to the application. The Reviewing Officer must be an employee and suitability qualified.

The review must be completed as soon as is reasonably practicable in the circumstances. If the review is not completed within **60 days** of the lodgement, the applicant is entitled to seek external review.

The Council must notify the Privacy Commissioner of an application as soon as practicable after its receipt, keep the Commissioner informed of the progress of the application and inform the Commissioner of the findings of the review and of the action it proposes to take in relation to the application.

The Privacy Commissioner is entitled to make submissions in relation to internal reviews and the council is required to consider any relevant material submitted by the Privacy Commissioner. The Council must provide the Privacy Commissioner with a draft of the council's internal review report to enable the Privacy Commissioner to make a submission.

Council may provide a copy of any submission by Privacy Commissioner's to the applicant.

The Council must notify the applicant of the outcome of the review within **14 days** of its determination. A copy of the final review should also be provided to the Privacy Commissioner where it departs from the draft review.

An internal review checklist has been prepared by the Office of the Privacy Commissioner NSW and can be accessed from its website http://www.ipc.nsw.gov.au .

The Privacy Commissioner must be notified of a complaint, briefed on progress and notified of the outcome of an internal review under the PPIPA or HRIPA.

What happens after an Internal Review?
If the complaint remains unsatisfied, he/she may appeal the Administrative Decisions Tribunal, which hears the matter afresh and may impose its own decision and can make a range of orders including an award of damages for a breach of an information protection principle or health privacy principle.

Other Relevant Matters

Contracts with consultants and other private contractors
It is necessary to have specific provisions to protect the Council in any dealings with private contractors.

Confidentiality
The obligation of confidentiality is additional to and separate from that of privacy. Nevertheless, a duty to withhold information lies at the heart of both concepts. Confidentiality attaches to information per se, personal or health information to the person to whom that information relates.

An obligation of confidentiality exists for all employees whether express or implied as a matter of law.

Information which may be confidential is also likely to have a separate and independent obligation of confidentiality will not suffice for privacy purposes. Two separate releases will be required and, in the case of privacy, the person to whom the information relates will be required to provide the release.

Misuse of personal or health information
Section 664 of the LGA makes it an offence for anyone to disclose information except in accordance with that section. Whether or not a particular disclosure is made with lawful excuse is a matter that requires legal opinion from case to case.

Regular review of the collection, storage and use of personal or health information
The information practices relating to the collection, storage and use of personal or health information will be reviewed by the Council every three (3) years. Any new program initiatives will be incorporated into the review process with a view to ascertaining whether or not those programs comply with the PPIPA.

Regular review of Privacy Management Plan
When information practices are reviewed from time to time, the Privacy Management Plan will also be reviewed to ensure that the Plan is up to date.

Further information
For assistance in understanding the processes under the PPIPA and HRIPA, please contact the Council or the Office of the Privacy Commissioner NSW on the details below:

Contact details

Privacy Officer
Bland Shire Council
PO Box 21
West Wyalong NSW 2671
Ph: 02 6972 2266
Email: council@blandshire.nsw.gov.au

Privacy Commissioner
GPO Box 7011
Sydney NSW 2001
Ph: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au

5. Definitions:

PIPPA: NSW Privacy and Personal Information Protection Act 1998
HRIPA: Health Records and Information Privacy Act 2002
GIPA: Government Information (Public Access) Act 2009

6. Legislation and Supporting Documents:

Privacy and Personal Information Protection Act 1998
Health Records Information and Privacy Act 2002
Government Information (Public Access) Act 2009
Government Information (Public Access) Act Regulation 2018
NSW Privacy and Personal Information Protection Act 1998
Local Government Act 1993
Environmental Planning and Assessment Act 1979
Protection of the Environment Operations Act 1997
Impounding Act 1993
State Records Act 1998
Health Practitioner Regulation National Law (NSW)
Privacy Code of Practice for Local Government
NSW Genetic Health Guidelines: Health Privacy Principles

7. Relationship to Community Strategic Plan:

This Policy supports Council's Delivery Program Strategy Strategy 12.4 - Review and implement Council policies and comply with WHS and Risk Management requirements.

8. Attachments:

- **Appendix 1 –** Information Protection Principles (IPPs)
- **Appendix 2 –** The Health and Privacy Principles (HPPs)

1 Appendix 1 - Information Protection Principles (IPPs)

Part 2, Division 1 of the PPIPA contains 12 Information Protection Principles with which we must comply.

1.1.1 Principle 1, Section 8 - Collection of personal information for lawful purposes

(1) A public sector agency must not collect personal information unless:
- *(a) The information is collected by for a lawful purpose that is directly related to a function or activity of the agency; and*
- *(b) The collection of the information is reasonably necessary for that purpose.*

(2) A public sector agency must not collect personal information by any unlawful means.

The Privacy Code of Practice for Local Government
There is no intention to depart from this principle.

1.1.2 Principle 2, Section 9 - Collection of personal information directly from individual

The public sector agency must, in collecting personal information, collect the information directly from the individual to whom the information relates unless:
- *(a) The individual has authorised collection of the information from someone else, or*
- *(b) In the case of information relating to a person who is under the age of 16 years – the information has been provided by a parent or guardian of the person.*

The Privacy Code of Practice for Local Government
Council is not required to comply with this principle where indirect collection of personal information is reasonably necessary when an award, prize, benefit or similar form of personal recognition is intended to be, or may be, conferred upon the person to whom the information relates.

1.1.3 Principle 3, Section 10 – Requirements when collecting personal information

If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances to ensure that, before the information is collected or as soon as practicable after collection, the individual to whom the information relates is made aware of the following:
- *(a) The fact that the information is being collected,*
- *(b) The purposes for which the information is being collected,*
- *(c) The intended recipients of the information,*
- *(d) Whether the supply of the information by the individual is required by law or is voluntary, and any consequences for the individual if the information (or any part of it) is not provided,*
- *(e) The existence of any right of access to, and correction of, the information,*
- *(f) The name and address of the agency that is collecting the information and the agency that is to hold the information.*

The Privacy Code of Practice for Local Government
Council may depart from this principle where indirect collection of personal information is reasonably necessary when an award, prize, benefit or similar form of personal recognition is intended to be, or may be, conferred upon the person to whom the information relates.

1.1.4 Principle 4, Section 11 – Other requirements relating to collection of personal information

If a public sector agency collects personal information from an individual, the agency 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 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.*

The Privacy Code of Practice for Local Government
There is no intention to depart from this principle.

1.1.5 Principle 5, Section 12 – Retention and security of personal information

A public sector agency that holds personal information must ensure:

(a) That the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used; and
(b) That the information is disposed of securely and in accordance with any requirements for the retention and disposal of personal information; and
(c) That 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) That, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of the information.

The Privacy Code of Practice for Local Government
There is no intention to depart from this principle.

1.1.6 Principle 6, Section 13 – Information about personal information held by agencies

A public sector agency that holds personal information must take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

(a) Whether the agency holds personal information; and
(b) Whether the agency holds personal information relating to that person; and
(c) If the agency holds personal information relating to that person:
  (i) The nature of that information; and
  (ii) The main purposes for which the information is used; and
  (iii) That person's entitlement to gain access to the information.

The Privacy Code of Practice for Local Government
There is no intention to depart from this principle.

1.1.7 Principle 7, Section 14 – Access to personal information held by agencies

A public sector agency that holds personal 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.

The Privacy Code of Practice for Local Government
There is no intention to depart from this principle.

1.1.8 Principle 8, Section 15 – Alteration of personal information

(1) A public sector agency that holds personal 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 personal 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 date, complete and not misleading.
(2) If a public sector agency is not prepared to amend personal information in accordance with a request by the individual to whom the information relates, the agency 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 personal information is amended in accordance with this section, 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 public sector agency.

(4) This section, and any provision of privacy code of practice that relates to the requirements set out in this section, apply to public sector agencies despite section 25 of this Act and Section 21 of the "State Records Act 1998".
(5) The Privacy Commissioner's guidelines under section 36 may make provision for or with respect to requests under this section, including the way in which such a request should be made and the time within which such a request should be dealt with.
*(6) In this section (and in any other provision of this Act in connection with the operation of this section), **public sector agency** includes a Minister and a Minister's personal staff.*

The Privacy Code of Practice for Local Government
There is no intention to depart from this principle.

1.1.9 Principle 9, Section 16 – Agency must check accuracy of personal information before use

A public sector agency that holds personal 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, up to date, complete and not misleading.

The Privacy Code of Practice for Local Government
There is no intention to depart from this principle.

1.1.10 Principle 10, Section 17 – Limits on use of personal information

A public sector agency that holds personal information must not use the information for a purpose other than that for which it as collected unless:
(a) The individual to whom the information relates has consented to the use of the information for that other purpose, or
(b) The other purpose for which the information is used is directly related to the purpose for which the information was collected, or
(c) The use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual tow whom the information relates or of another person.

The Privacy Code of Practice for Local Government
Council may use personal information for a purpose other than the purpose for which it was collected in the following circumstances:
(1) Where the use is for the purpose of undertaking Council's lawful and proper function/s and Council is satisfied that the personal information is reasonably necessary for the exercise of such function/s, or
(2) Where personal information is to be used for the purpose of conferring upon a particular person, an award, prize, benefit or similar form of personal recognition.

1.1.11 Principle 11, Section 18 – Limits on disclosure of personal information

(1) A public sector agency that holds personal information must not disclose the information to a person (other than the individual to whom the information relates) or other body, whether or not such other person or body is a public sector agency unless:
(a) The disclosure is directly related to the purpose for which the information was collected and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure, or
(b) The individual concerned is reasonably likely to have been aware, or has been made aware in accordance with section 10, that information of that kind is usually disclosed to that other person or body, or
(c) The agency believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person.

(2) If personal information is disclosed in accordance with subsection (1) to a person or body that is a public sector agency, that agency must not use or disclose the information for a purpose other than the purpose for which the information was given to it.

Appendix 1 – Information Protection Principles (IPPs)

The Privacy Code of Practice for Local Government

There is no intention to depart from this principle except in the circumstances described below:

(1) Council may disclose personal information to public sector agencies or utility providers on condition that:
- *(i) The agency or utility provider has approached Council in writing*
- *(ii) Council is satisfied that the information is to be used by that agency or utility provider for the proper and lawful function/s of that agency or utility provider, and*
- *(iii) Council is satisfied that the personal information is reasonably necessary for the exercise of that agency or utility provider's function/s.*

(2) Where personal information about an individual collected or held by Council is to be disclosed for the purpose of conferring upon that person, an award, prize, benefit or similar form of personal recognition.

(3) Where Council is requested by a potential employer, it may verify:
- *(i) That a current or former employee works or has worked for Council*
- *(ii) The duration of their employment, and*
- *(iii) The position occupied during their employment.*

This exemption shall not permit Council to give and opinion as to that person's suitability to a particular position with any potential employer unless Council is satisfied that the person has provided their consent for Council to provide a reference, which may include an opinion as to that person's suitability for the position for which he/she has applied.

1.1.12 Principle 12, Section 19 – Special restrictions on disclosure of personal information

(1) A public sector agency must not disclose personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, sexual activities unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or another person.

(2) A public sector agency that holds personal information must not disclose the information to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless:
- *(a) A relevant privacy law that applies to the personal information concerned is in force in that the jurisdiction or applies to that Commonwealth agency, or*
- *(b) The disclosure is permitted under a privacy code of practice.*

(3) For the purposes of subsection (2), a relevant privacy law means a law that is determined by the Privacy Commissioner, by notice published in the Gazette, to be a privacy law for the jurisdiction concerned.

(4) The Privacy Commissioner is to prepare a code relating to the disclosure of personal information by public sector agencies to persons or bodies outside New South Wales and the Commonwealth agencies.

(5) Subsection (2) does not apply:
- *(a) Until after the first anniversary of the commencement of this section, or*
- *(b) Until a code referred to in subsection (4) is made,*

Whichever is the later.

The Privacy Code of Practice for Local Government

There is no intention to depart from this principle except in the circumstances described below:

(1) For the purposes of section 19(2), where Council is requested by a potential employer outside New South Wales, it may verify that:
- *(i) A current or former employee works or has worked for Council*
- *(ii) The duration of their employment, and*
- *(iii) The position occupied during their employment*

This exemption shall not permit Council to give an opinion as to that person's suitability for a particular position with any potential employer unless Council is satisfied that the person has provided their consent for Council to provide a reference, which may include an opinion as to that person's suitability for the position for which he/she has applied.

2 Appendix 2 - The Health Privacy Principles (HPPs)

Under the provisions of the *Health Records and Information Privacy Act, 2002 (HRIPA)* Council has a legal obligation in how it must collect, hold use and disclose individual's health information.

The following is a list of examples of the types of health information and circumstances in which Council may collect health information:

- Seniors' bus outings where information may be collected on special medical needs;
- Information on carers and families for the purposes of children's services;
- Volunteer programs where volunteers are asked to disclose health conditions which assist Council to provide support in the event of an incident or which may preclude them from some types of volunteer work;
- Information in relation to the need for assisted waste services; and
- Information relating to employee health for example, pre-employment medical declarations, medical certificates and workers' compensation.

In the same way as the Information Privacy Principles that have been outlined above, the provisions of HRIPA allow for Health Privacy Principles. The meaning, intent and application of these principles are required when handling health information.

The Health Information Principles and the Information Privacy Principles are very similar with some principles overlapping in areas. For more information on the Health Privacy Principles, refer to the Information and Privacy Commissioner: www.ipc.nsw.gov.au .

2.1.1 Principle 1 – 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.

2.1.2 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 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 of the personal affairs of the individual to whom the information relates.

2.1.3 Principle 3 – Collection to be from individual concerned

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

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

2.1.4 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 that 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 types 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 pose 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 NSW 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 is necessarily implied or reasonably contemplated) under an 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 an 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.

2.1.5 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 for 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 the organisation is done to prevent 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 Stat Records Act 1998).

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

2.1.6 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 organisations hold health information relating to that individual; and*
- *(c) If the organisation holds health information relating to that individual:*
  - *(i) The nature of that information; and*
  - *(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 an Act or any other law (including the State Records Act 1998).*

2.1.7 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).*

2.1.8 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 date, 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 individual 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;
(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).

2.1.9 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, up to date, complete and not misleading.

2.1.10 Principle 10 – Limits on use of health information

*(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 or public safety; or
*(c1) **Genetic information:** the information is genetic information and the use of the information for the secondary purpose:*
(i) Is reasonably believed by the organisation to be necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat is imminent) of a genetic relative of the individual to whom the genetic information relates; and
(ii) Is in accordance with guidelines, if any, issued by the NSW Privacy Commissioner for the purposes of this paragraph; 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'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 NSW 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 NSW 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) 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 NSW Privacy Commissioner for the purposes of this paragraph; or

(g) ***Find missing person:*** *the information for the secondary purpose is by law enforcement agency (or such other person 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:***

(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 been in conduct that may be unsatisfactory professional conduct or professional misconduct under 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

(i) 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 circumstance 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 f 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 in 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.

2.1.11 Principle 11 – Limits on disclosure of health information

*(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 an 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

*(c1) **Genetic information:** the information is genetic information and the disclosure of the information for the secondary purpose:*

(i) Is reasonably believed by the organisation to be necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat is imminent) of a genetic relative of the individual to whom the genetic information relates; and

(ii) Is in accordance with guidelines, if any, issued by the NSW Privacy Commissioner for the purposes of this paragraph; 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 individual, 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 NSW 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 individual, 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 NSW 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) If the information could reasonably be expected to identify individual, 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 NSW Privacy Commissioner for the purposes of this paragraph; or

*(g) **Compassionate reasons:** the disclosure of the information for the secondary purpose is to provide 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 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 insufficient 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 been or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under 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.

2.1.12 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.*

2.1.13 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.

2.1.14 Principle 14 – Transborder data flows and data flows 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:

(1) 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

(2) The individual consents to the transfer, or

(3) 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

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

(5) 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*

(6) 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

(7) 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

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

2.1.15 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 (10 (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.*