

DOCUMENT TYPE:	Council policy
DOCUMENT STATUS:	Approved
POLICY OWNER POSITION:	Director Corporate
INTERNAL COMMITTEE ENDORSEMENT:	Management Executive Group
APPROVED BY:	Council
DATE ADOPTED:	23/01/2024
VERSION NUMBER:	3
REVIEW DATE:	23/01/2026
DATE RESCINDED:	
RELATED STRATEGIC DOCUMENTS, POLICIES OR PROCEDURES:	Cloud Computing Policy Records Management Policy Website Privacy Statement Complaint Handling Framework
RELATED LEGISLATION:	<i>Victoria</i> Privacy and Data Protection Act 2014 Health Records Act 2001 Local Government Act 2020 Freedom of Information Act 1982 Public Records Act 1973  <i>Commonwealth</i> Privacy Act 1988

EVIDENCE OF APPROVAL:



---

Signed by Chief Executive Officer

FILE LOCATION: K:\EXECUTIVE\Strategies policies and procedures\Policies - adopted PDF and Word\POL Privacy Policy v3.docx

**Policy documents are amended from time to time, therefore you should not rely on a printed copy being the current version. Please consult the policies on the Loddon Shire website (Council Policies) or Intranet (Organisational Policies) to ensure that the version you are using is up to date.**

**This document is available in alternative formats (e.g. larger font) if requested.**

## 1 PURPOSE

This policy explains how the Loddon Shire Council (Council) will collect, hold, use and disclose the personal and health information of individuals, how individuals can gain access to their information and correct inaccuracies, and how an individual may complain about possible breaches of privacy.

The purpose of this policy is to:

- help individuals understand how Council handles their information
- help employees understand how personal information should be handled
- prevent the unnecessary collection or unlawful use or disclosure of information, and
- promote greater public confidence in Council's handling of personal information.

## 2 SCOPE

This policy covers all personal and/or health information held by Council, including information that Council has collected:

- from an individual, as well as information sourced from or provided by third parties
- about an individual in any format including correspondence, in person, over the phone, over the internet, or from third parties.

## 3 POLICY

Council is committed to protecting individuals' right to privacy and to the responsible and fair handling of personal and/or health information, consistent with the *Privacy and Data Protection Act 2014* (PDP Act), and the *Health Records Act 2014* (HR Act).

Accordingly, Council will adhere to the Information Privacy Principles (IPP) and Health Privacy Principles (HPP) when undertaking its statutory functions and activities, so that the privacy of individuals can be protected (for further information on the IPP and HPP see Attachment 1 – Information Privacy Principles, and Attachment 2 – Health Privacy Principles respectively).

### 3.1 What are privacy rights?

It is important that individuals are aware of their privacy rights under the PDP Act and the HR Act and the *Privacy Act 1988* and know what to do if there is a problem.

Individuals have the right to:

- know why an organisation is asking for their information and what they are going to do with it
- ask to see their own information and request corrections if necessary, and
- make a complaint if they believe their personal information has been mishandled.

### 3.2 What types of information does Council collect?

The types of personal, sensitive and health information that Council may collect includes but is not limited to name, address, email address, telephone number, date of birth, motor vehicle registration, photograph or video footage, disabilities, pension card numbers, bank account and other financial details of residents, ratepayers and staff.

Council will only collect personal information (including sensitive and health information) that is necessary for its functions and activities.

## 3.3 How does Council manage information?

### 3.3.1 Collection (IPP 1/HPP 1)

Council will collect personal and/or health information, lawfully and fairly, that is necessary for carrying out its functions and activities:

- directly from the individual via an application form or correspondence or in response to a request from Council
- from third parties, such as contracted service providers, health service providers or the individual's authorised representatives or legal advisers
- from publicly available sources of information
- when legally required to do so.

When collecting personal or health information Council will endeavour to:

- take reasonable steps to advise what and why the information is being collected
- disclose to whom the information may be disclosed and why
- disclose any law that requires Council to collect the information
- advise the consequences for the individual if all or part of the information is not collected
- advise the individual that they are able to gain access to the information.

Where possible and appropriate, this will be achieved by a Collection Notice which will also let individuals know how they can access their information. Prior to commencing collection, a Privacy Impact Assessment<sup>1</sup> may be undertaken by staff.

Council will maintain a Website Privacy Statement on its website which will outline how privacy is managed for users who access the website.

Council will not collect sensitive or health related information unless the individual has consented or it is required by law.

Council will take reasonable steps to retain confidentiality of any personal information about an individual, given by another person or a health service provider, in relation to the provision of care or health services to the individual.

If Council collects personal and/or health information about an individual from someone else, it will take reasonable steps (such as calling the individual to confirm personal information) to ensure that the individual is made aware of it.

Council will collect personal and/or health information about a child under the age of 18, only with the consent of the child's parent or guardian. However in certain circumstances Council may exercise discretion in obtaining parental/guardian consent for the collection of young persons' information where parental/guardian involvement may hinder the delivery of services to a young person.

---

<sup>1</sup> Refer to the Office of the Victorian Information Commission for further information on how to conduct a Privacy Impact Assessment (<https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-officer-toolkit/privacy-impact-assessments/>)

Council may collect personal and/or health information for purposes including, but not limited to, the following:

- to contact an individual where it is necessary in order to provide services requested by them, such as obtaining a permit
- as part of our commitment to customer service, we may periodically invite individuals to provide feedback about their experience via a survey, any survey is voluntary and you do not have to participate
- for Council or our contracted service providers to contact you where it is necessary to resolve issues relating to Council services or functions which the individual has brought to our attention, for instance, contacting an individual in response to their report of a fallen tree branch
- to contact an individual prior to a Council or Committee meeting to confirm attendance and/or advise of any changes to the meeting details where the individual has made a submission for consideration
- to supply material concerning Council initiatives and programs where personal information has been supplied to Council for this purpose, for instance, where an individual has opted to be included on a mailing list for a Council publication via our public interfaces
- to facilitate the collection of Council fees and charges, for instance, we will use name and address details to forward rate notices
- to enable payment for Council provided goods and services
- to enable Council to undertake its law enforcement functions
- to aid community safety
- to record/receive ideas, questions, complaints, and compliments from members of the public.

### 3.3.2 Use and Disclosure (IPP 2/HPP 2)

Council will take all necessary measures to prevent unauthorised access to, or disclosure of, an individual's personal information.

Council will only use personal and/or health information within Council, or disclose it outside Council for the purpose for which it was collected and in accordance with legislation (e.g. where the individual has consented or where the individual would reasonably expect this to occur).

Use includes:

- searching records for any reason
- using personal and/or health information in a record to make a decision
- inserting personal and/or health information into a database.

Disclosure includes:

- providing personal and/or health information to a third party (such as a contractor)
- providing a record containing personal and/or health information to a member of the public
- providing access to public registers Council is required to maintain.

External organisations to which personal information is disclosed include Council's contracted service providers who perform various services for and on behalf of Council. These contractors have agreed to be bound by the provisions of the PDP Act. Information provided to these contractors is limited to contact details.

Council will not disclose personal or health information to a third party without consent, unless Council is required or authorised to do so by law. In the event of an investigation into suspected unlawful or improper activity, a law enforcement agency or government agency may exercise its legal authority to request information and inspect records.

Council may be required to forward contact details to government departments and agencies, utility companies, and other agencies and businesses including but not limited to:

- Powercor
- Coliban Water
- Goulburn Murray Water
- GWM Water
- State Government departments
- Neighbouring Councils
- Public Records Office Victoria
- Victoria Police
- VicRoads/Regional Roads Victoria

All above mentioned departments, agencies and Councils are required to comply with privacy legislation.

As far as is reasonably practicable, disclosures of personal information will be made in writing and recorded in Council's records management system.

### 3.3.3 Data Quality (IPP 3/HPP 3)

Prior to the use and disclosure of personal and/or health information, reasonable steps will be taken to ensure that the information is relevant and to the extent necessary, accurate, complete and up-to-date for the purpose for which it is to be used.

### 3.3.4 Data Security (IPP 4) and Data Security and Data Retention (HPP 4)

Council will endeavour to maintain a secure system for storing personal and/or health information and will utilise appropriate technologies, security methods, operational policies and procedures to protect the information from:

- unauthorised access
- improper use
- alteration
- unlawful or accidental destruction
- accidental loss.

All personal and/or health information will be managed in accordance with the HR Act and the *Public Records Act 1973*.

The Victorian Protective Data Security Framework (VPDSF), and accompanying Victorian Protective Data Security Standards (VPDSS), provide direction to Victorian public sector agencies or bodies on their data security obligations. The VPDSS establish 12 high level mandatory requirements to protect public sector information across all security areas including governance, information, personnel, information communications technology and physical security.

### 3.3.5 Openness (IPP 5/ HPP 5)

Council will take reasonable steps to ensure a person knows what personal and health information it holds, for what purposes and how it is managed.

### 3.3.6 Access and Correction (IPP 6/HPP 6)

Following the collection of personal information, the individual whose information has been collected may contact Council for access to that information.

Access will be provided except in the circumstances outlined in the PDP Act, for example, where the information relates to legal proceedings or where the *Freedom of Information Act 1982* applies.

If it is established that information held by Council is inaccurate, incomplete, misleading or not up to date, Council will take reasonable steps to correct the information.

Council will provide written reasons for refusal of access to, or refusal to correct health information.

### 3.3.7 Identifiers (IPP 7/HPP 7)

Council will only assign identifiers to records if it is necessary to enable Council to carry out a function efficiently.

Council will not adopt as its own identifier for an individual any unique identifier that has been assigned by another government agency.

Council will not use or disclose the identifier assigned to an individual by another government agency, unless the consent of the individual has been obtained or it is required by law to do so.

### 3.3.8 Anonymity (IPP 8/HPP 8)

Whenever it is lawful and practicable, individuals may exercise the option of not identifying themselves when supplying information or entering into transactions with Council.

Some Council services can only be provided if the person accessing the service is prepared to be identified due to practical and legal requirements

### 3.3.9 Transborder Data Flows (IPP 9/HPP 9)

Council may transfer personal and/or health information about an individual to someone (other than Council or the individual) who is outside Victoria when the data transfer conforms with the PDP Act and/or the HR Act.

Council will take all reasonable steps to ensure that the information which it transfers will not be held, used or disclosed by the host of the information in a manner inconsistent with Commonwealth or Victorian privacy legislation.

### 3.3.10 Sensitive Information (IPP 10)

Council will not collect sensitive information about you except in circumstances prescribed in the PDP Act.

### 3.3.11 Transfer or closure of the practice of a health service provider (HPP 10)

If Council sells or closes down a health service it will publish a notice of its intent to do so and take steps to notify any individual of whom it holds health information. Council will transfer records as required under the HR Act.

### 3.3.12 Making information available to another health service provider (HPP 11)

Council will make information available to another health service provider if requested to do so by an individual. Fees may be applicable.

### 3.4 Privacy Complaints

An individual may lodge a complaint in writing with Council's Privacy Officer regarding the handling of personal and/or health information. Council will investigate and deal with the complaint in accordance with Council's Complaint Handling Framework.

Council's Privacy Officer contact details:

Privacy Officer  
Loddon Shire Council  
PO Box 21,  
WEDDERBURN VIC 3518  
  
Telephone: (03) 5494 1200  
Email: [loddon@loddon.vic.gov.au](mailto:loddon@loddon.vic.gov.au)

Alternatively an individual can make a complaint to an independent regulator of privacy which may conciliate privacy complaints between aggrieved parties:

Office of the Victorian Information Commissioner  
PO Box 24274  
MELBOURNE VIC 3001

Telephone: 1300 006 842

Email: [enquiries@ovic.vic.gov.au](mailto:enquiries@ovic.vic.gov.au)

Website: [www.ovic.vic.gov.au](http://www.ovic.vic.gov.au)

or

Health Complaints Commissioner  
Level 26, 570 Bourke Street  
MELBOURNE VIC 3000

Telephone: 1300 582 113

Email: [hcc@hcc.vic.gov.au](mailto:hcc@hcc.vic.gov.au)

Website [www.hcc.vic.gov.au](http://www.hcc.vic.gov.au)

The Commissioners may decline to action the complaint if the complainant has not first complained to Council.

### 3.5 Further information

Copies of this policy will be readily available from the Council website and office.

Further information with respect to the Loddon Shire Council's Privacy Policy and its handling of personal and/or health information can be obtained from Council's Privacy Officer.

## 4 DEFINITIONS OF TERMS OR ABBREVIATIONS USED

Term	Definition
Collection notice	a statement that is provided to an individual at or before the time Council collects personal information (or if that is not practical, as soon as possible after the information is collected). A collection notice explains to individuals the purpose for which the information is collected, and how the organisation will use and handle the information.
Health information	<p>Health information means—</p> <ul style="list-style-type: none"> <li>(a) information or an opinion about— <ul style="list-style-type: none"> <li>(i) the physical, mental or psychological health (at any time) of an individual; or</li> <li>(ii) a disability (at any time) of an individual; or</li> <li>(iii) an individual's expressed wishes about the future provision of health services to him or her; or</li> <li>(iv) a health service provided, or to be provided, to an individual—</li> </ul> <p>that is also personal information; or</p> </li> <li>(b) other personal information collected to provide, or in providing, a health service; or</li> <li>(c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or</li> <li>(d) other personal information that is genetic information about an individual in a form which is or could be predictive of the health (at any time) of the individual or of any of his or her descendants—</li> </ul> <p>but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of this Act generally or for the purposes of specified provisions of this Act;</p> <p>Health information is legislated under the HR Act, and administered by the Health Complaints Commissioner.</p>
HPPs	Health Privacy Principles, found in the <i>Health Records Act 2001</i>
Identifier	a number, letter or symbol or a combination of any or all of those things, that may be used to identify an individual or to verify the identity of an individual.
IPPs	Information Privacy Principles found in the <i>Privacy and Data Protection Act 2014 (Vic)</i>

Term	Definition
Personal information	<p>Personal information is defined in the PDP Act as:</p> <p>information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the Health Records Act 2001 applies;</p> <p>Personal information is information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained from the information or opinion but does not include information of a kind to which the HR Act applies.</p> <p>Personal information may include:</p> <ul style="list-style-type: none"> <li>• name, age, height, weight</li> <li>• income, purchases and spending habits</li> <li>• bank account details and credit card information</li> <li>• photographs</li> <li>• blood type</li> <li>• fingerprints</li> <li>• marital status</li> <li>• religious belief</li> <li>• education</li> <li>• home address and phone number</li> <li>• employee details</li> <li>• information about an individual opinion and what an individual likes</li> <li>• Medicare number</li> <li>• motor vehicle registration number</li> </ul> <p>Personal information is and administered by the Victorian Information Commissioner.</p>
Privacy Impact Assessment	<p>a process that helps identify, assess, and mitigate the impact a program may have on the privacy of individuals. It helps organisations consider the different elements of the proposed program, how it may involve the handling of personal information, and any inherent privacy risks.</p>
Public registers	<p>documents that Councils are required to make publically available pursuant to State Government legislation</p>

Term	Definition
Sensitive information	Sensitive is a subset of personal information, it is defined in the PDP Act as information or an opinion about an individual's— <ul style="list-style-type: none"> <li>(a) racial or ethnic origin; or</li> <li>(b) political opinions; or</li> <li>(c) membership of a political association; or</li> <li>(d) religious beliefs or affiliations; or</li> <li>(e) philosophical beliefs; or</li> <li>(f) membership of a professional or trade association; or</li> <li>(g) membership of a trade union; or</li> <li>(h) sexual preferences or practices; or</li> <li>(i) criminal record—</li> </ul> that is also personal information
Unique identifier	means an identifier (usually a number) assigned by an organisation to an individual uniquely to identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name but does not include an identifier within the meaning of the Health Records Act 2001.
Office of the Victorian Information Commissioner	the primary regulator and source of independent advice to the community and Victorian government about how the public sector collects, uses and discloses information.

## 5 HUMAN RIGHTS STATEMENT

It is considered that this policy does not impact negatively on any rights identified in the Charter of Human Rights Act. Loddon Shire Council is committed to consultation and cooperation between management and employees. The Council will formally involve elected employee Health and Safety Representatives in any workplace change that may affect the health and safety of any of its employees.

## 6 REVIEW

The Director Corporate will review this policy for any necessary amendments no later than 2 years after adoption of this current version. The Director Corporate may approve updates to the appendices of this policy at any time.

## 7 APPENDICES

- 1) Information Privacy Principles
- 2) Health Privacy Principles

## 8 APPENDIX 1 THE INFORMATION PRIVACY PRINCIPLES (IPP)

### Privacy and Data Protection Act 2014

---

#### Schedule 1—The Information Privacy Principles

In these Principles—

**sensitive information** means information or an opinion about an individual's—

- (a) racial or ethnic origin; or
- (b) political opinions; or
- (c) membership of a political association; or
- (d) religious beliefs or affiliations; or
- (e) philosophical beliefs; or
- (f) membership of a professional or trade association; or
- (g) membership of a trade union; or
- (h) sexual preferences or practices; or
- (i) criminal record—

that is also personal information;

**unique identifier** means an identifier (usually a number) assigned by an organisation to an individual uniquely to identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual's name and does not include an identifier within the meaning of the **Health Records Act 2001**.

#### 1 Principle 1—Collection

- 1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.
- 1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.
- 1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of—
  - (a) the identity of the organisation and how to contact it; and
  - (b) the fact that the individual is able to gain access to the information; and
  - (c) the purposes for which the information is collected; and
  - (d) to whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind; and
  - (e) any law that requires the particular information to be collected; and
  - (f) the main consequences (if any) for the individual if all or part of the information is not provided.
- 1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

- 1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in IPP 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

## 2 Principle 2—Use and Disclosure

- 2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless—
- (a) both of the following apply—
    - (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;
    - (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or
  - (b) the individual has consented to the use or disclosure; or
  - (c) if the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest, other than for publication in a form that identifies any particular individual—
    - (i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and
    - (ii) in the case of disclosure—the organisation reasonably believes that the recipient of the information will not disclose the information; or
  - (d) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent—
    - (i) a serious threat to an individual's life, health, safety or welfare; or
    - (ii) a serious threat to public health, public safety or public welfare; or
  - (e) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
  - (f) the use or disclosure is required or authorised by or under law; or
  - (g) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of a law enforcement agency—
    - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction;
    - (ii) the enforcement of laws relating to the confiscation of the proceeds of crime;
    - (iii) the protection of the public revenue;
    - (iv) the prevention, detection, investigation or remedying of seriously improper conduct;
    - (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or

(h) the Australian Security Intelligence Organisation (ASIO) or the Australian Secret Intelligence Service (ASIS), in connection with its functions, has requested the organisation to disclose the personal information and—

- (i) the disclosure is made to an officer or employee of ASIO or ASIS (as the case requires) authorised in writing by the Director-General of ASIO or ASIS (as the case requires) to receive the disclosure; and
- (ii) an officer or employee of ASIO or ASIS (as the case requires) authorised in writing by the Director-General of ASIO or ASIS (as the case requires) for the purposes of this paragraph has certified that the disclosure would be connected with the performance by ASIO or ASIS (as the case requires) of its functions.

2.2 If an organisation uses or discloses personal information under IPP 2.1(g), it must make a written note of the use or disclosure.

### **3 Principle 3—Data Quality**

3.1 An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date.

### **4 Principle 4—Data Security**

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

### **5 Principle 5—Openness**

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

### **6 Principle 6—Access and Correction**

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that—

- (a) providing access would pose a serious threat to the life or health of any individual; or
- (b) providing access would have an unreasonable impact on the privacy of other individuals; or
- (c) the request for access is frivolous or vexatious; or
- (d) the information relates to existing legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery or subpoena in those proceedings; or
- (e) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
- (f) providing access would be unlawful; or

- (g) denying access is required or authorised by or under law; or
  - (h) providing access would be likely to prejudice an investigation of possible unlawful activity; or
  - (i) providing access would be likely to prejudice—
    - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction; or
    - (ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or
    - (iii) the protection of public revenue; or
    - (iv) the prevention, detection, investigation or remedying of seriously improper conduct; or
    - (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders—by or on behalf of a law enforcement agency; or
  - (j) ASIO, ASIS or a law enforcement agency performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.
- 6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.
- 6.3 If the organisation is not required to provide the individual with access to the information because of one or more of IPP 6.1(a) to (j) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.
- 6.4 If an organisation charges for providing access to personal information, the organisation—
- (a) must advise an individual who requests access to personal information that the organisation will provide access on the payment of the prescribed fee; and
  - (b) may refuse access to the personal information until the fee is paid.
- 6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up to date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up to date.
- 6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up to date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up to date, the organisation must take reasonable steps to do so.
- 6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.
- 6.8 If an individual requests access to, or the correction of, personal information held by an organisation, the organisation must—
- (a) provide access, or reasons for the denial of access; or

- (b) correct the personal information, or provide reasons for the refusal to correct the personal information; or
- (c) provide reasons for the delay in responding to the request for access to or for the correction of personal information—

as soon as practicable, but no later than 45 days after receiving the request.

## 7 Principle 7—Unique Identifiers

- 7.1 An organisation must not assign unique identifiers to individuals unless the assignment of unique identifiers is necessary to enable the organisation to carry out any of its functions efficiently.
- 7.2 An organisation must not adopt as its own unique identifier of an individual a unique identifier of the individual that has been assigned by another organisation unless—
  - (a) it is necessary to enable the organisation to carry out any of its functions efficiently; or
  - (b) it has obtained the consent of the individual to the use of the unique identifier; or
  - (c) it is an outsourcing organisation adopting the unique identifier created by a contracted service provider in the performance of its obligations to the organisation under a State contract.
- 7.3 An organisation must not use or disclose a unique identifier assigned to an individual by another organisation unless—
  - (a) the use or disclosure is necessary for the organisation to fulfil its obligations to the other organisation; or
  - (b) one or more of IPP 2.1(d) to (g) applies to the use or disclosure; or
  - (c) it has obtained the consent of the individual to the use or disclosure.
- 7.4 An organisation must not require an individual to provide a unique identifier in order to obtain a service unless the provision of the unique identifier is required or authorised by law or the provision is in connection with the purpose (or a directly related purpose) for which the unique identifier was assigned.

## 8 Principle 8—Anonymity

- 8.1 Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering into transactions with an organisation.

## 9 Principle 9—Transborder Data Flows

- 9.1 An organisation may transfer personal information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if—
  - (a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Information 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 precontractual 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 that consent, the individual would be likely to give it; or
- (f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Information Privacy Principles.

## 10 Principle 10—Sensitive Information

10.1 An organisation must not collect sensitive information about an individual unless—

- (a) the individual has consented; or
- (b) the collection is required or authorised under law; or
- (c) the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual whom the information concerns—
  - (i) is physically or legally incapable of giving consent to the collection; or
  - (ii) physically cannot communicate consent to the collection; or
- (d) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite IPP 10.1, an organisation may collect sensitive information about an individual if—

- (a) the collection—
  - (i) is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or
  - (ii) is of information relating to an individual's racial or ethnic origin and is collected for the purpose of providing government funded targeted welfare or educational services; and
- (b) there is no reasonably practicable alternative to collecting the information for that purpose; and
- (c) it is impracticable for the organisation to seek the individual's consent to the collection.

## 9 APPENDIX 2 THE HEALTH PRIVACY PRINCIPLES

### Health Records Act 2001

---

#### Schedule 1—The Health Privacy Principles

##### 1 Principle 1—Collection

###### *When health information may be collected*

- 1.1 An organisation must not collect health information about an individual unless the information is necessary for one or more of its functions or activities and at least one of the following applies—
- (a) the individual has consented;
  - (b) the collection is required, authorised or permitted, whether expressly or impliedly, by or under law (other than a prescribed law);
  - (c) the information is necessary to provide a health service to the individual and the individual is incapable of giving consent within the meaning of section 85(3) and—
    - (i) it is not reasonably practicable to obtain the consent of an authorised representative of the individual within the meaning of section 85; or
    - (ii) the individual does not have such an authorised representative;
  - (d) the information is disclosed to the organisation in accordance with HPP 2.2(a), (f), (i) or (l) or HPP 2.5;
  - (e) if the collection is necessary for research, or the compilation or analysis of statistics, in the public interest—
    - (i) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and
    - (ii) it is impracticable for the organisation to seek the individual's consent to the collection; and
    - (iii) the information is collected in accordance with guidelines issued or approved by the Health Complaints Commissioner under section 22 for the purposes of this subparagraph;
  - (f) the collection is necessary to prevent or lessen—
    - (i) a serious threat to the life, health, safety or welfare of any individual; or
    - (ii) a serious threat to public health, public safety or public welfare—and the information is collected in accordance with guidelines, if any, issued or approved by the Health Complaints Commissioner under section 22 for the purposes of this paragraph;
  - (g) the collection is by or on behalf of a law enforcement agency and the organisation reasonably believes that the collection is necessary for a law enforcement function;
  - (h) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim;

- (i) the collection is in the prescribed circumstances.

### ***How health information is to be collected***

- 1.2 An organisation must collect health information only by lawful and fair means and not in an unreasonably intrusive way.
- 1.3 If it is reasonable and practicable to do so, an organisation must collect health information about an individual only from that individual.
- 1.4 At or before the time (or, if that is not practicable, as soon as practicable thereafter) an organisation collects health information about an individual from the individual, the organisation must take steps that are reasonable in the circumstances to ensure that the individual is generally aware of—
  - (a) the identity of the organisation and how to contact it; and
  - (b) the fact that he or she is able to gain access to the information; and
  - (c) the purposes for which the information is collected; and
  - (d) to whom (or the types of individuals or organisations to which) the organisation usually discloses information of that kind; and
  - (e) any law that requires the particular information to be collected; and
  - (f) the main consequences (if any) for the individual if all or part of the information is not provided.
- 1.5 If an 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 or has been made aware of the matters listed in HPP 1.4 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual or would involve the disclosure of information given in confidence.
- 1.6 An organisation is not required to notify the individual of the identity of persons, or classes of persons, to whom health information may be disclosed in accordance with HPP 2.2(f).

### ***Information given in confidence***

- 1.7 If personal information is given in confidence to a health service provider about an individual by a person other than—
  - (a) the individual; or
  - (b) a health service provider in the course of, or otherwise in relation to, the provision of health services to the individual—

with a request that the information not be communicated to the individual to whom it relates, the provider must—

- (c) confirm with the person that the information is to remain confidential; and
- (d) if the information remains confidential—
  - (i) record the information only if it is relevant to the provision of health services to, or the care of, the individual; and
  - (ii) take reasonable steps to ensure that the information is accurate and not misleading; and
- (e) take reasonable steps to record that the information is given in confidence and is to remain confidential.

## 2 Principle 2—Use and Disclosure

- 2.1 An organisation may use or disclose health information about an individual for the primary purpose for which the information was collected in accordance with HPP 1.1.
- 2.2 An organisation must not use or disclose health information about an individual for a purpose (the **secondary purpose**) other than the primary purpose for which the information was collected unless at least one of the following paragraphs applies —
- (a) both of the following apply—
    - (i) the secondary purpose is directly related to the primary purpose; and
    - (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or
  - (b) the individual has consented to the use or disclosure; or
  - (c) the use or disclosure is required, authorised or permitted, whether expressly or impliedly, by or under law (other than a prescribed law); or
  - (d) all of the following apply—
    - (i) the organisation is a health service provider providing a health service to the individual; and
    - (ii) the use or disclosure for the secondary purpose is reasonably necessary for the provision of the health service; and
    - (iii) the individual is incapable of giving consent within the meaning of section 85(3) and—
      - (A) it is not reasonably practicable to obtain the consent of an authorised representative of the individual within the meaning of section 85; or
      - (B) the individual does not have such an authorised representative; or
  - (e) all of the following apply—
    - (i) the organisation is a health service provider providing a health service to the individual; and
    - (ii) the use is for the purpose of the provision of further health services to the individual by the organisation; and
    - (iii) the organisation reasonably believes that the use is necessary to ensure that the further health services are provided safely and effectively; and
    - (iv) the information is used in accordance with guidelines, if any, issued or approved by the Health Complaints Commissioner under section 22 for the purposes of this paragraph; or
  - (f) the use or disclosure is for the purpose of—
    - (i) funding, management, planning, monitoring, improvement or evaluation of health services; or
    - (ii) training provided by a health service provider to employees or persons working with the organisation—and—
    - (iii) that purpose cannot be served by the use or 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 individual's consent to the use or disclosure; or

- (iv) reasonable steps are taken to de-identify the information—  
and—
  - (v) 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
  - (vi) the information is used or disclosed in accordance with guidelines, if any, issued or approved by the Health Complaints Commissioner under section 22 for the purposes of this subparagraph; or
- (g) if the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest—
  - (i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and
  - (ii) that purpose cannot be served by the use or disclosure of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and
  - (iii) the use or disclosure is in accordance with guidelines issued or approved by the Health Complaints Commissioner under section 22 for the purposes of this subparagraph; and
  - (iv) in the case of disclosure—
    - (A) the organisation reasonably believes that the recipient of the health information will not disclose the health information; and
    - (B) the disclosure will not be published in a form that identifies particular individuals or from which an individual's identity can reasonably be ascertained; or
- (h) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent—
  - (i) a serious threat to an individual's life, health, safety or welfare; or
  - (ii) a serious threat to public health, public safety or public welfare—  
and the information is used or disclosed in accordance with guidelines, if any, issued or approved by the Health Complaints Commissioner under section 22 for the purposes of this paragraph; or
- (i) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities and, if the organisation is a registered health practitioner, the use or disclosure would not be a breach of confidence; or
- (j) the organisation reasonably believes that the use or disclosure is reasonably necessary for a law enforcement function by or on behalf of a law enforcement agency and, if the organisation is a registered health practitioner, the use or disclosure would not be a breach of confidence; or
- (k) the use or disclosure is necessary for the establishment, exercise or defence of a legal or equitable claim; or
- (l) the use or disclosure is in the prescribed circumstances.

## Note

Nothing in HPP 2 requires an organisation to disclose health information about an individual. An organisation is always entitled not to disclose health information in the absence of a legal obligation to disclose it.

- 2.3 If an organisation discloses health information under paragraph (i) or (j) of HPP 2.2, it must make a written note of the disclosure.
- 2.4 Despite HPP 2.2, a health service provider may disclose health information about an individual to an immediate family member of the individual if—
- (a) either—
    - (i) the disclosure is necessary to provide appropriate health services to or care of the individual; or
    - (ii) the disclosure is made for compassionate reasons; and
  - (b) the disclosure is limited to the extent reasonable and necessary for the purposes mentioned in paragraph (a); and
  - (c) the individual is incapable of giving consent to the disclosure within the meaning of section 85(3); and
  - (d) the disclosure is not contrary to any wish—
    - (i) expressed by the individual before the individual became incapable of giving consent and not changed or withdrawn by the individual before then; and
    - (ii) of which the organisation is aware or could be made aware by taking reasonable steps; and
  - (e) in the case of an immediate family member who is under the age of 18 years, considering the circumstances of the disclosure, the immediate family member has sufficient maturity to receive the information.
- 2.5 Despite HPP 2.2, an organisation may use or disclose health information about an individual where—
- (a) it is known or suspected that the individual is dead; or
  - (b) it is known or suspected that the individual is missing; or
  - (c) the individual has been involved in an accident or other misadventure and is incapable of consenting to the use or disclosure—
- and the use or disclosure is to the extent reasonably necessary—
- (d) to identify the individual; or
  - (e) to ascertain the identity and location of an immediate family member or other relative of the individual for the purpose of—
    - (i) enabling a police officer, a coroner or other prescribed organisation to contact the immediate family member or other relative for compassionate reasons; or
    - (ii) to assist in the identification of the individual—
- and, in the circumstances referred to in paragraph (b) or (c)—
- (f) the use or disclosure is not contrary to any wish—

- (i) expressed by the individual before he or she went missing or became incapable of consenting and not withdrawn by the individual; and
  - (ii) of which the organisation is aware or could have become aware by taking reasonable steps; and
- (g) the information is used or disclosed in accordance with guidelines, if any, issued or approved by the Health Complaints Commissioner under section 22 for the purposes of this paragraph.

### **3 Principle 3—Data Quality**

3.1 An organisation must take steps that are reasonable in the circumstances to make sure that, having regard to the purpose for which the information is to be used, the health information it collects, uses, holds or discloses is accurate, complete, up to date and relevant to its functions or activities.

### **4 Principle 4—Data Security and Data Retention**

4.1 An organisation must take reasonable steps to protect the health information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 A health service provider must not delete health information relating to an individual, even if it is later found or claimed to be inaccurate, unless—

- (a) the deletion is permitted, authorised or required by the regulations or any other law; or
- (b) the deletion is not contrary to the regulations or any other law and occurs—
  - (i) in the case of health information collected while the individual was a child, after the individual attains the age of 25 years; or
  - (ii) in any case, more than 7 years after the last occasion on which a health service was provided to the individual by the provider—

whichever is the later.

4.3 A health service provider who deletes health information in accordance with HPP 4.2 must make a written note of the name of the individual to whom the health information related, the period covered by it and the date on which it was deleted.

4.4 A health service provider who transfers health information to another individual or organisation and does not continue to hold a record of that information must make a written note of the name and address of the individual or organisation to whom it was transferred.

4.5 An organisation other than a health service provider must take reasonable steps to destroy or permanently de-identify health information if it is no longer needed for the purpose for which it was collected or any other purpose authorised by this Act, the regulations made under this Act or any other law.

### **5 Principle 5—Openness**

5.1 An organisation must set out in a document—

- (a) clearly expressed policies on its management of health information; and
- (b) the steps that an individual must take in order to obtain access to their health information.

The organisation must make the document available to anyone who asks for it.

5.2 On request by an individual, an organisation must take reasonable steps—

- (a) to let the individual know—
  - (i) whether the organisation holds health information relating to the individual; and
  - (ii) the steps that the individual should take if the individual wishes to obtain access to the information; and
- (b) if the organisation holds health information relating to the individual, to let the individual know in general terms—
  - (i) the nature of the information; and
  - (ii) the purposes for which the information is used; and
  - (iii) how the organisation collects, holds, uses and discloses the information.

## 6 Principle 6—Access and Correction

### Access

- 6.1 If an organisation holds health information about an individual, it must provide the individual with access to the information on request by the individual in accordance with Part 5, unless—
- (a) providing access would pose a serious threat to the life or health of any person under section 26 and refusing access is in accordance with guidelines, if any, issued or approved by the Health Complaints Commissioner under section 22 for the purposes of this paragraph; or
  - (b) providing access would have an unreasonable impact on the privacy of other individuals and refusing access is in accordance with guidelines, if any, issued or approved by the Health Complaints Commissioner under section 22 for the purposes of this paragraph; or
  - (c) the information relates to existing legal proceedings between the organisation and the individual and the information would not be accessible by the process of discovery in those proceedings or is subject to legal professional privilege or client legal privilege; or
  - (d) providing access would reveal the intentions of the organisation in relation to negotiations, other than about the provision of a health service, with the individual in such a way as to expose the organisation unreasonably to disadvantage; or
  - (e) the information is subject to confidentiality under section 27; or
  - (f) providing access would be unlawful; or
  - (g) denying access is required or authorised by or under law; or
  - (h) providing access would be likely to prejudice an investigation of possible unlawful activity; or
  - (i) providing access would be likely to prejudice a law enforcement function by or on behalf of a law enforcement agency; or
  - (j) a law enforcement agency performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia; or
  - (k) the request for access is of a kind that has been made unsuccessfully on at least one previous occasion and there are no reasonable grounds for making the request again; or

(l) the individual has been provided with access to the health information in accordance with Part 5 and is making an unreasonable, repeated request for access to the same information in the same way.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than access to the information.

### **Note**

An organisation breaches HPP 6.1 if it relies on HPP 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where HPP 6.2 does not apply.

6.3 If access is refused on the ground that it would pose a serious threat to the life or health of the individual, the procedure in Division 3 of Part 5 applies.

6.4 Without limiting sections 26 and 27, nothing in this Principle compels an organisation to refuse to provide an individual with access to his or her health information.

### **Correction**

6.5 If an organisation holds health information about an individual and the individual is able to establish that the information is inaccurate, incomplete, misleading or not up to date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up to date but must not delete the information otherwise than in accordance with HPP 4.2.

6.6 If—

- (a) the organisation is not willing to correct the health information in accordance with a request by the individual; and
- (b) no decision or recommendation to the effect that the information should be corrected wholly or partly in accordance with the request, is pending or has been made under this Act or any other law; and
- (c) the individual gives to the organisation a written statement concerning the requested correction—

the organisation must take reasonable steps to associate the statement with the information.

6.7 If the organisation accepts the need to correct the health information but—

- (a) the organisation considers it likely that leaving incorrect information, even if corrected, could cause harm to the individual or result in inappropriate health services or care being provided; or
- (b) the form in which the health information is held makes correction impossible; or
- (c) the corrections required are sufficiently complex or numerous for a real possibility of confusion or error to arise in relation to interpreting or reading the record if it were to be so corrected—

the organisation must place the incorrect information on a record which is not generally available to anyone involved in providing health services to the individual, and to which access is restricted, and take reasonable steps to ensure that only the corrected information is generally available to anyone who may provide health services to the individual.

- 6.8 If an organisation corrects health information about an individual, it must—
- (a) if practicable, record with the correction the name of the person who made the correction and the date on which the correction is made; and
  - (b) take reasonable steps to notify any health service providers to whom the organisation disclosed the health information before its correction and who may reasonably be expected to rely on that information in the future.
- 6.9 If an individual requests an organisation to correct health information about the individual, the organisation must take reasonable steps to notify the individual of a decision on the request as soon as practicable but in any case not later than 30 days after the request is received by the organisation.

### ***Written reasons***

- 6.10 An organisation must provide written reasons for refusal of access or a refusal to correct health information.

## **7 Principle 7—Identifiers**

- 7.1 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.
- 7.2 Subject to HPP 7.4, a private sector organisation may only adopt as its own identifier of an individual an identifier of an individual that has been assigned by a public sector organisation (or by an agent of, or contractor to, a public sector organisation 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.
- 7.3 Subject to HPP 7.4, a private sector organisation may only use or disclose an identifier assigned to an individual by a public sector organisation (or by an agent of, or contractor to, a public sector organisation 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 of paragraphs (c) to (l) of HPP 2.2; or
  - (b) the individual has consented to the use or disclosure; or
  - (c) the disclosure is to the public sector organisation which assigned the identifier to enable the public sector organisation to identify the individual for its own purposes.
- 7.4 If the use or disclosure of an identifier assigned to an individual by a public sector organisation is necessary for a private sector organisation to fulfil its obligations to, or requirements of, the public sector organisation, a private sector organisation may either—
- (a) adopt as its own identifier of an individual an identifier of the individual that has been assigned by the public sector organisation; or
  - (b) use or disclose an identifier of the individual that has been assigned by the public sector organisation.

## **8 Principle 8—Anonymity**

- 8.1 Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

## 9 Principle 9—Transborder Data Flows

- 9.1 An organisation may transfer health information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if—
- (a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which 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 that consent, the individual would be likely to give it; or
  - (f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Health Privacy Principles; or
  - (g) the transfer is authorised or required by any other law.

## 10 Principle 10—Transfer or closure of the practice of a health service provider

- 10.1 This Principle applies if the practice or business of a health service provider (*the provider*) is to be—
- (a) sold or otherwise transferred and the provider will not be providing health services in the new practice or business; or
  - (b) closed down.
- 10.2 The provider or, if the provider is deceased, the legal representatives of the provider, must—
- (a) publish a notice in a newspaper circulating in the locality of the practice or business stating—
    - (i) that the practice or business has been, or is about to be, sold, transferred or closed down, as the case may be; and
    - (ii) the manner in which the provider proposes to deal with the health information held by the practice or business about individuals who have received health services from the provider, including whether the provider proposes to retain the information or make it available for transfer to those individuals or their health service providers; and
  - (b) take any other steps to notify individuals who have received a health service from the provider in accordance with guidelines issued or approved by the Health Complaints Commissioner under section 22 for the purposes of this paragraph.

- 10.3 Not earlier than 21 days after giving notice in accordance with HPP 10.2, the person giving the notice must, in relation to health information about an individual held by, or on behalf of, the practice or business, elect to retain that information or transfer it to—
- (a) the health service provider, if any, who takes over the practice or business; or
  - (b) the individual or a health service provider nominated by him or her.
- 10.4 A person who elects to retain health information must continue to hold it or transfer it to a competent organisation for safe storage in Victoria, until the time, if any, when the health information is destroyed in accordance with HPP 4.
- 10.5 Subject to HPP 10.2, a person must comply with the requirements of this Principle as soon as practicable.
- 10.6 Despite any other provision of the Health Privacy Principles, a person who transfers health information in accordance with this Principle does not, by so doing, contravene the Health Privacy Principles.
- 10.7 If—
- (a) an individual, in response to a notice published under HPP 10.2, requests that health information be transferred to him or her or to a health service provider nominated by him or her; and
  - (b) the person who published the notice elects to retain the health information—
- the request must be taken to be—
- (c) in the case of a request that the health information be transferred to him or her, a request for access to that health information in accordance with Part 5 or HPP 6; and
  - (d) in the case of a request that the health information be transferred to a health service provider nominated by him or her, a request for the transfer of that health information in accordance with HPP 11—
- and it must be dealt with in accordance with this Act.
- 10.8 This Principle operates subject to any other law, including the **Public Records Act 1973**.
- 10.9 For the purposes of HPP 10.1(a), a business or practice of a provider is transferred if—
- (a) it is amalgamated with another organisation; and
  - (b) the successor organisation which is the result of the amalgamation is a private sector organisation.

## **11 Principle 11—Making information available to another health service provider**

- 11.1 If an individual—
- (a) requests a health service provider to make health information relating to the individual held by the provider available to another health service provider; or
  - (b) authorises another health service provider to request a health service provider to make health information relating to the individual held by that provider available to the requesting health service provider—
- a health service provider to whom the request is made and who holds health information about the individual must, on payment of a fee not exceeding the

prescribed maximum fee and subject to the regulations, provide a copy or written summary of that health information to that other health service provider.

- 11.2 A health service provider must comply with the requirements of this Principle as soon as practicable.
- 11.3 Nothing in Part 5 or HPP 6 limits the operation of this Principle.
- 11.4 For the purposes of HPP 10.7, this Principle applies to a legal representative of a deceased health service provider in the same way that it applies to a health service provider.