Suas Rov Pty Limited

Privacy guidelines and procedure

Joseph McMahon
June 2019

Table of Contents

SUAS ROV PTY LIITED

Privacy Guidelines and Procedure

SECTION 1 - INTRODUCTION

PURPOSE

To establish guidelines that must be observed by all Suas Rov Pty Limited ("SuasRov") staff in relation to the collection, use, storage, security and disclosure of personal information, sensitive information and health records.

SCOPE

These guidelines apply company wide.

LEGISLATIVE CONTEXT

Name	Location
Privacy Act (Cwth.)1988	http://www.comlaw.gov.au/
Privacy Amendment (Enhancing Privacy Protection) Act 2012	http://www.austlii.edu.au/cgi-bin/sinodisp/au/legis/cth/num_act/pappa2012466/index.html#sch1
Privacy Act (Cwth.) 1988 - Draft APP Guidelines	http://www.oaic.gov.au/privacy/privacy-engaging-with-you/previous-privacy-consultations/draft-australian-privacy-principles-guidelines/draft-app-guidelines
Information Privacy Act (Vic.) 2000	http://www.legislation.vic.gov.au/Domino/Web_Notes/LDMS/LTObject_Store/LTObjSt6.nsf/DDE300B846EED9C7CA257616000A3571/A9DCDED8F32066EFCA2578E600090FF8/$FILE/00-98aa022%20authorised.pdf
Information Privacy Act (Vic.) 2000 - Guidelines	http://www.privacy.vic.gov.au/
Health Records Act (Vic.) 2001	http://www.legislation.vic.gov.au/Domino/Web_Notes/LDMS/LTObject_Store/LTObjSt6.nsf/DDE300B846EED9C7CA257616000A3571/77FAA53ECDC0DA44CA2579030015D701/$FILE/01-2aa023%20authorised.pdf
Freedom of Information Act (Vic.) 1982	http://www.legislation.vic.gov.au/Domino/Web_Notes/LDMS/LTObject_Store/LTObjSt6.nsf/DDE300B846EED9C7CA257616000A3571/8D77927CC7483A8BCA257A290021C292/$FILE/82-9859aa071%20authorised.pdf
Public Records Act (Vic.) 1973	http://www.legislation.vic.gov.au/Domino/Web_Notes/LDMS/LTObject_Store/LTObjSt6.nsf/DDE300B846EED9C7CA257616000A3571/D2B93E4380A5627

SECTION 2 - GUIDELINES

Privacy Guidelines

Part 1	General

1.1 General Principles

Interpretation:

In these *Company Privacy Guidelines* the following applies:

'APP' means *Australian Privacy Principle*. Australian Privacy Principles have been established under the Commonwealth's *Privacy Act 1988*. There are 13 *APPs*.

'IPP' means *Information Privacy Principle*. Information Privacy Principles have been established under the Victorian *Information Privacy Act 2000*.There are 10 *IPPs*.

'HPP' means *Health Privacy Principle*. Health Privacy Principles have been established under the Victorian *Health Records Act 2001*. There are 11 *HPPs*.

Note 1: The number following the *APP*, *IPP* or *HPP* reference is a reference to the particular principle bearing that number.

Note 2: The full texts of the *APPs*, the *IPPs and the HPPs* are set out in ***Appendix 1*** to these *Company Privacy Guidelines*.

These ***Suas Rov Pty Limited Privacy Guidelines*** (the "*Company Privacy Guidelines*") establish and maintain:

- a regime for the responsible collection and management of personal information by Suas Rov in a way that is open and transparent;
- a regime for reasonable steps to be taken by Suas Rov to implement measures that will ensure the Company complies with the Commonwealth's *Australian Privacy Principles*, the Victorian *Information Privacy Principles* and the Victorian *Health Privacy Principles* (collectively called "the *Privacy Principles'*);
- a regime that will enable Suas Rov to deal with inquiries or complaints regarding the Company's compliance with the *Privacy Principles*;
- a regime that will enable Suas Rov to have and maintain a clearly expressed and up-to-date privacy policy regarding the management of personal information by the Company; and
- a regime that, amongst other things, addresses the following matters:
  - the kinds of personal information that Suas Rov collects and holds;
  - how Suas Rov collects and holds personal information;
  - the purposes for which Suas Rov collects, holds, uses and discloses

personal information;

- how an individual may access personal information about the individual that is held by Suas Rov and how that individual may seek the correction of such information;
- how an individual may complain about a breach of the *Australian Privacy Principles*, or any of the other *Privacy Principles* applicable to Suas Rov, and how Suas Rov will deal with such a complaint;
- whether Suas Rov is likely to disclose personal information to overseas recipients;
- if Suas Rov is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the *Company Privacy Guidelines.*

1.2 Definitions

Note 1: Privacy Victoria, (the statutory body administering the *Information Privacy Act (2000)*) has produced guidelines and determinations that clarify the definitions used in the *Information Privacy Act* http://www.privacy.vic.gov.au/ The definitions set out below draw on the definitions applicable in Victoria, but they have been adjusted where necessary in an effort to comply with the Victorian *Health Records Act 2001* and the Commonwealth's requirements under the Commonwealth *Privacy Act 1988 (as amended)*.

Note 2: References to "*this Act*", "*sections*", or "*sub-sections*" are, where the context permits, references to the *Privacy Act,* or sections or sub-sections of that *Act*.

Australian law means:

(a) an Act of the Commonwealth or of a State or Territory; or

(b) regulations, or any other instrument, made under such an Act; or

(c) a Norfolk Island enactment; or

(d) a rule of law or equity.

Collects Suas Rov ***collects*** personal information only if it collects the personal information for inclusion in a record or *generally available publication*.

Compliance Officer The ***Compliance Officer*** will be responsible for the administration of the *Company Privacy Guidelines*.

Specifically, the Compliance Officer will:

(a) keep records which are required to be kept under this Policy; and

(b) inform and assist staff with respect to privacy issues.

Generally Available Publication means a magazine, book, newspaper or other publication (however published) that is or will be generally available to members of the public and includes information held on a public register.

Genetic relative of an individual ***(the first individual)*** means another individual who is related to the first individual by blood, including but not limited to a sibling, a parent or a descendant of the first individual.

Health information *means personal information about an individual that includes:*

(a) Information or an opinion about-

(i) the physical, mental or psychological health (at any time) of an individual; or

(ii) a disability (at any time) of an individual; or

(iii) an individual's expressed wishes about the future provision of health services to him or her; or

(iv) a health service provided, or to be provided, to an individual; or

(b) Other personal information collected to provide, or in providing, a health service; or

(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

(d) Other personal information that is genetic information about an individual in a form that is, or could be, predictive of the health (at any time) of the individual or of any of his or her genetic relatives.

Note 1: **"*health information*" *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 specified provisions of the *Health Records Act*.

Note 2: The terms a "*permitted general situation*" and a "*permitted health situation*" are relevant to general and health information.

Health Service means:

(a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the organisation or the person performing it-

(i) to assess, record, maintain or improve the individual's health; or

(ii) to diagnose the individual's illness, injury or disability; or

(iii) to treat the individual's illness, injury or disability or suspected illness, injury or disability; or

(b) a disability service, palliative care service or aged care service; or

(c) the dispensing on prescription of a drug or medicinal preparation by a pharmacist; or

(d) a service, or a class of service, provided in conjunction with an activity or service referred to in paragraph (a), (b) or (c) that is prescribed as a health service.

Note 1: The reference to a "***health service***" ***does not include*** a health service, or a class of health service, that is prescribed (or to the extent that it is prescribed) as an exempt health service for the purposes of specified provisions of the *Health Records Act.*

Health Service Provider means an organisation that provides a health service in Victoria. Suas Rov's health service providers include, but are not limited to, the Health / Medical Service and the Counselling Services.

Note 2: Under the *Privacy Act*, the concept of a "***permitted health situation***" is relevant to the interpretation of the term "***health service provider***". The *Privacy Act* refers to an organisation that provides a health service as one that has obligations of professional confidentiality that bind the organisation in accordance with rules established by competent health and medical bodies.

Holds Suas Rov "***holds***" personal information if it has possession or control of a record that contains the personal information, notwithstanding that such possession or control is alone or jointly with other persons or bodies, and irrespective of where the record is situated, whether in or outside Victoria.

Identifier An "***identifier***" of an individual means a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify the identity of the individual, but does not include:

(a) the individual's name; or

(b) the individual's ABN (within the meaning of the *A New Tax System (Australian Business Number) Act 1999*); or

(c) anything else prescribed by the (*Privacy Act*) regulations;

and ***de-identified*** personal information is "***de-identified***" if the information is no longer about an identifiable individual or an individual who is reasonably identifiable;

and a "***government related identifier***" of an individual means an identifier of the individual that has been assigned by:

(a) an agency; or

(b) a State or Territory authority; or

(c) an agent of an agency, or a State or Territory authority, acting in its capacity as agent; or

(d) a contracted service provider for a Commonwealth contract, or a State contract, acting in its capacity as contracted service provider for that contract.

Permitted General Situation

(1) A ***permitted general situation*** exists in relation to the collection, use or disclosure by an *APP* entity of personal information about an individual, or of a government related identifier of an individual, if:

(a) the entity is an entity of a kind specified in an item in column 1 of the table; and

(b) the item in column 2 of the table applies to the information or identifier; and

(c) such conditions as are specified in the item in column 3 of the table are satisfied.

Permitted general situations

Item	Column 1 Kind of entity	Column 2 Item applies to	Column 3 Condition(s)
1	APP entity	(a) personal information; or (b) a government related identifier.	(a) it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure; and (b) the entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.
2	APP entity	(a) personal information; or (b) a government related identifier.	(a) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in; and (b) the entity reasonably believes that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter.
3	APP entity	Personal information	(a) the entity reasonably believes that the collection, use or disclosure is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing; and (b) the collection, use or disclosure complies with the rules made under subsection (2).
4	APP entity	Personal information	The collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim.
5	APP entity	Personal information	The collection, use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution process.
6	Agency	Personal information	The entity reasonably believes that the collection, use or disclosure is necessary for the entity's diplomatic or consular functions or activities.
7	Defence Force	Personal information	The entity reasonably believes that the collection, use or disclosure is necessary for any of the following occurring outside Australia and the external Territories: (a) war or warlike operations; (b) peacekeeping or peace enforcement; (c) civil aid, humanitarian assistance, medical or civil emergency or disaster relief.

Note: The Commonwealth's Information Commissioner may, by legislative instrument, make rules relating to the collection, use or disclosure of personal information that apply for the purposes of item 3 of the table in the above subsection (1).

Permitted Health Situation

There are 5 '***permitted health situations'*** defined in the *APPs*:

(1) A ***permitted health situation*** exists in relation to the collection by an organisation of health information about an individual if:

(a) the information is necessary to provide a health service to the individual; and

(b) either:

(i) the collection is required or authorised by or under an Australian law (other than this Act); or

(ii) the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

Collection—research etc.

(2) A ***permitted health situation*** exists in relation to the collection by an organisation of health information about an individual if:

(a) the collection is necessary for any of the following purposes:

(i) research relevant to public health or public safety;

(ii) the compilation or analysis of statistics relevant to public health or public safety;

(iii) the management, funding or monitoring of a health service; and

(b) that purpose cannot be served by the collection of information about the individual that is *de-identified* information; and

(c) it is impracticable for the organisation to obtain the individual's consent to the collection; and

(d) any of the following apply:

(i) the collection is required by or under an *Australian law* (other than this *Act*);

(ii) the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation;

(iii) the information is collected in accordance with guidelines approved under *section 95A* for the purposes of this subparagraph.

Use or disclosure—research etc.

(3) A ***permitted health situation*** exists in relation to the use or disclosure by an organisation of *health information* about an individual if:

(a) the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety; and

(b) it is impracticable for the organisation to obtain the individual's consent to the use or disclosure; and

(c) the use or disclosure is conducted in accordance with guidelines approved under *section 95A* for the purposes of this paragraph; and

(d) in the case of disclosure—the organisation reasonably believes that the recipient of the information will not disclose the information, or *personal information* derived from that information.

Use or disclosure—genetic information

(4) A ***permitted health situation*** exists in relation to the use or disclosure by an organisation of genetic information about an individual (the *first individual*) if:

(a) the organisation has obtained the information in the course of providing a *health service* to the first individual; and

(b) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the first individual; and

(c) the use or disclosure is conducted in accordance with guidelines approved under *section 95AA*; and

(d) in the case of disclosure—the recipient of the information is a *genetic relative* of the first individual.

Disclosure—responsible person for an individual

(5) A ***permitted health situation*** exists in relation to the disclosure by an organisation of *health information* about an individual if:

(a) the organisation provides a *health service* to the individual; and

(b) the recipient of the information is a responsible person for the individual; and

(c) the individual:

(i) is physically or legally incapable of giving consent to the disclosure; or

(ii) physically cannot communicate consent to the disclosure; and

(d) another individual (the ***carer***) providing the *health service* for the organisation is satisfied that either:

(i) the disclosure is necessary to provide appropriate care or treatment of the individual; or

(ii) the disclosure is made for compassionate reasons; and

(e) the disclosure is not contrary to any wish:

(i) expressed by the individual before the individual became unable to give or communicate consent; and

(ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and

(f) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (d).

Personal Information means information or an opinion (including information or an opinion forming part of a database), about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.

Primary Purpose means the purpose for which the individual concerned should expect his or her information to be used. Using the information for this purpose should be within his or her reasonable expectations as the purpose would be necessary, or directly related to, one or more of Suas Rov's functions or activities.

Note 1: The main functions of Suas Rov are to provide teaching and research services, together with ancillary services, which may support students and staff in their study or work at the Company. Further, some information is required to be collected by Suas Rov for governmental purposes. Suas Rov considers the aforementioned functions and requirements as the factors underlying the *primary purpose* for the collection of the *personal information*.

Note 2: The purpose for which *health information* is collected by Suas Rov is set out in the following table:

Company Department/ Unit	**Purpose of Collection of Health Information**
Medical Service	Provision of physical, mental and psychological health services
Counselling Services	Provision of psychological support services
Academic Units/ Research Centres	Undertaking of Research
Academic Units/Other Company Divisions	As supporting documentation for verification purposes

Record includes a '*document*', an electronic or other device (including a database (however kept), a photograph or other pictorial representation of a person, personal information, health information, sensitive information [or any combination of such information]) regarding an individual.

A record may include such things as factual data (e.g. name, student ID number,

address, telephone number, age, enrolment status, employment details, digital image etc.), details of academic progress (e.g. course details, examination results, evaluation and assessment, academic standing etc.) and personal welfare information (e.g. emergency contacts, family matters, medical matters and financial matters)-

but a '*record*' does not include:

(a) a generally available publication; or

(b) anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition; or

(c) Commonwealth records as defined by subsection 3(1) of the *Archives Act 1983* that are in the open access period for the purposes of that Act; or

(d) records (as defined in the *Archives Act 1983*) in the care (as defined in that Act) of the National Archives of Australia in relation to which the Archives has entered into arrangements with a person other than a Commonwealth institution (as defined in that Act) providing for the extent to which the Archives or other persons are to have access to the records; or

(e) documents placed by or on behalf of a person (other than an agency) in the memorial collection within the meaning of the *Australian War Memorial Act 1980* ; or

(f) letters or other articles in the course of transmission by post; or

(g) a public record under the control of the Keeper of Public Records that is available for public inspection in accordance with the *Public Records Act 1973 (Victoria)*; or

(h) archives within the meaning of the *Copyright Act 1968* of the Commonwealth.

Note: A "***document***" means any record of information, and includes:

(a) anything on which there is writing; and

(b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; and

(c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else; and

(d) a map, plan, drawing or photograph.

Responsible Person

(1) A ***responsible person*** for an individual is:

(a) a parent of the individual; or

(b) a child or sibling of the individual if the child or sibling is at least 18 years old; or

(c) a spouse or de facto partner of the individual; or

(d) a relative of the individual if the relative is:

(i) at least 18 years old; and

(ii) a member of the individual's household; or

(e) a guardian of the individual; or

(f) a person exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or

(g) a person who has an intimate personal relationship with the individual; or

(h) a person nominated by the individual to be contacted in case of emergency.

(2) In this *section*:

child: without limiting who is a child of an individual for the purposes of *subsection (1)*, each of the following is a ***child*** of an individual:

(a) an adopted child, stepchild, exnuptial child or foster child of the individual;

(b) someone who is a child of the individual within the meaning of the *Family Law Act 1975*.

parent: without limiting who is a parent of an individual for the purposes of *subsection (1)*, someone is a ***parent*** of an individual if the individual is his or her child because of the definition of ***child*** in this *subsection*.

relative of an individual (the ***first individual***) means a grandparent, grandchild, uncle, aunt, nephew or niece of the first individual and for this purpose, relationships to the first individual may also be traced to or through another individual who is:

(a) a de facto partner of the first individual; or

(b) the child of the first individual because of the definition of child in this *subsection*.

sibling of an individual includes:

(a) a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister of the individual; and

(b) another individual if a relationship referred to in paragraph (a) can be traced through a parent of either or both of the individuals.

stepchild: without limiting who is a stepchild of an individual, someone is a ***stepchild*** of an individual if he or she would be the individual's stepchild except that the individual is not legally married to the individual's de facto partner.

Secondary Purpose means a purpose other than the *primary purpose*. The secondary purpose may or may not be apparent to the individual concerned, or within his or her reasonable expectations. The main distinction is that the service provided by Suas Rov could still be provided even if the secondary purpose were not served.

Sensitive Information means information or an opinion about an individual's:

(a) (i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual orientation or practices; or

(ix) criminal record;

that is also *personal information*; or

(b) *health information* about an individual; or

(c) genetic information about an individual that is not otherwise *health information*; or

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

(e) biometric templates.

1.3 Availability of *Company Privacy Guidelines* etc.

Suas Rov makes its *Company Privacy Guidelines* available on its website free of charge. The website address is:

https://www.suasrov.com.au

If a person or body requests a copy of the *Company Privacy Guidelines* in a particular form Suas Rov will take such steps as are reasonable in the circumstances to make its *Company Privacy Guidelines* available free of charge in such other form as may be appropriate.

Suas Rov intends that these *Company Privacy Guidelines* are expressed in terms that can be reasonably understood. If any person or body has difficulty in understanding anything contained in these *Company Privacy Guidelines* or, if any person or body believes the clarity of these *Company Privacy Guidelines* might be improved, then Suas Rov invites that person or body to contact the Company's Privacy Officer (the "Privacy Officer").

The contact details for Suas Rov's Privacy Officer are as follows:

Joseph McMahon

(+61) 0408 953 713

jmcmahon@suasrov.com.au

Note: See also section 12 of these *Company Privacy Guidelines* (*Access to, and correction of, personal information*).

2 3 Anonymity and pseudonymity

An individual has the option of not identifying him or herself, or of using a pseudonym, when dealing with Suas Rov in relation to a particular matter.

However, if, in relation to a particular matter –

(a) Suas Rov is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or

(b) it is impracticable for Suas Rov to deal with individuals who have not identified themselves or who have used a pseudonym –

then an individual in such circumstances may not be permitted the option of not identifying him or herself, or of using a pseudonym, when dealing with Suas Rov in relation to that particular matter.

Part 2 Collection of personal information

Suas Rov will only collect personal information (other than *sensitive* information) that is necessary for, or directly related to, one or more of Suas Rov's functions or activities.

Note 1: Section 19-60 and clause 23 of Schedule 1A of the *Higher Education Support Act* (*HESA*) 2003 (Commonwealth) require a higher education provider and a VET provider to comply with the *Privacy Act (Commonwealth),* the Higher Education Provider Guidelines, and the VET Guidelines, relating to personal information in relation to students. Suas Rov must also comply with the relevant requirements of the *Information Privacy Principles* set out in the *Information Privacy Act 2000 (Victoria)* and the *Health Privacy Principles* set out in the *Health Records Act 2001 (Victoria)*.

Note 2: Sensitive information is subject to special provisions under these *Company Privacy Guidelines.* In particular, please see sections 3, 6 and 7 of these *Company Privacy Guidelines* below.

Personal information Suas Rov collects may either be "***solicited***" or "***unsolicited***".

"***Solicited***" personal information is personal information that Suas Rov expressly requests regarding the individual concerned. The request may be addressed to the individual concerned, or to another person or an entity. The request may be to provide

the personal information or to provide a kind of information in which that personal information is included.

"***Unsolicited***" personal information is personal information coming to Suas Rov that Suas Rov did not request.

Note 3: *Personal information* that Suas Rov collects from staff, students, prospective students, past students, benefactors, research participants, and external contractors includes:

- Names
- Student Identification Numbers
- Addresses
- Emergency Contacts
- Photographic Identification
- Other related *personal information* required for the effective management of the Company

3 Collection of *solicited* personal information

Note: *Section 3.1* and *3.2* only apply to the collection of *personal information* that is solicited by Suas Rov.

3.1 Collection of *solicited* personal information that is *sensitive* information

Sensitive information

3.1.1 Suas Rov will not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information, and the information is reasonably necessary for, or directly related to, one or more of Suas Rov's functions or activities; or

(b) 3.1.2 applies in relation to the information:

3.1.2 The following applies in relation to sensitive information about an individual if:

(a) the collection of the information is required or authorised by or under an *Australian law* or a court / tribunal order; or

(b) a *permitted general situation* exists in relation to the collection of the information by Suas Rov; or

(c) a *permitted health situation* exists in relation to the collection of the information by Suas Rov.

Note 1: '*Sensitive information'* includes '*health information'*.

Note 2: Please see the '*Definitions*' section in 1.2 of these *Company Privacy Guidelines* for the meanings of '*a permitted general situation'* and '*a permitted health situation'*.

Note 3: Suas Rov is permitted to collect '*health information*' where that 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)* of the *Health Records Act 2001* and it is not reasonably practicable to obtain the consent of an authorised representative of the individual within the meaning of section 85, or, the individual does not have such an authorised representative.

Note 4: The *Health Records Act 2001* falls within the definition of an *Australian law*.

Note 5: **Information given in confidence**

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.

3.2 Means of collection

3.2.1 Suas Rov will only collect personal information by lawful and fair means.

3.2.2 Suas Rov will only collect personal information about an individual from the individual unless:

(a) the individual consents to the collection of the information from someone other than the individual; or

(b) Suas Rov is required or authorised by or under an *Australian law*, or a court / tribunal order, to collect the information from someone other than the individual; or

(c) it is unreasonable or impracticable to do so.

Note: With reference to 3.2.2 (b), and by way of providing some examples, Suas Rov will sometimes collect personal information from entities such as VTAC, or a temporary employment agency, or a contractor. Where Suas Rov collects information about an individual, Suas Rov will generally take reasonable steps to ensure that the individual is made aware of the personal information it has collected (see 5.1 and 5.2 below).

4 Dealing with *unsolicited* personal information

4.1 If Suas Rov receives personal information which it did not request, then within a reasonable period after receiving the information, Suas Rov will determine whether or not it could have collected the information if it had requested it under the rules relating to

the collection of solicited information under section 3 above.

4.2 Suas Rov may use or disclose the unsolicited personal information for the purpose of making the determination referred to in section 4.1.

4.3 If Suas Rov determines that it *could not have* collected the personal information under the rules relating to the collection of solicited information, and, if the information is not contained in a Commonwealth record, then, Suas Rov will, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

4.4 If Suas Rov determines that it *could have* collected the personal information under the rules relating to the collection of solicited information, then Suas Rov will treat the information in the same way as if it had collected it under the rules relating to the collection of solicited information, and accordingly, the relevant parts of these *Company Privacy Guidelines* will apply to such information.

5 Notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, Suas Rov collects personal information about an individual, Suas Rov will take such steps (if any) as are reasonable in the circumstances:

(a) to notify the individual of such matters referred to in section 5.2 of this *Company Privacy Policy* below as are reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of any such matters.

Note 1: Suas Rov is not required to make the individual aware of the collection of the *health information* if, by making the individual aware of such matters, it would pose a serious threat to the life or health of any individual or would involve the disclosure of information given in confidence.

Note 2: Suas Rov is not required to notify the individual of the identity of persons, or a class of persons, to whom *health information* may be disclosed if the use or disclosure is associated with a particular *permitted health situation* and complies with any relevant guidelines.

5.2 The matters for the purposes of section 5.1 of this *Company Privacy Policy* above are as follows:

(a) the identity and contact details of Suas Rov;

(b) if:

(i) Suas Rov collects the personal information from someone other than the individual; or

(ii) the individual may not be aware that Suas Rov has collected the personal information;

the fact that Suas Rov so collects, or has collected, the information and the circumstances of that collection;

(c) if the collection of the personal information is required or authorised by or under an *Australian law* or a court / tribunal order—the fact that the collection is so required or authorised (including the name of the *Australian law*, or details of the court / tribunal order, that requires or authorises the collection);

(d) the purposes for which Suas Rov collects the personal information;

(e) the main consequences (if any) for the individual if all or some of the personal information is not collected by Suas Rov;

(f) any other agency, organisation, body or person, or the types of any other, agency, organisation, bodies or persons, to which Suas Rov usually discloses personal information of the kind collected by Suas Rov;

(g) that the *Company Privacy Guidelines* of Suas Rov contains information about how the individual may access the personal information about the individual that is held by Suas Rov and seek the correction of such information;

(h) that the *Company Privacy Guidelines* of Suas Rov contains information about how the individual may complain about a breach of the *Australian Privacy Principles* that bind Suas Rov, and how Suas Rov will deal with such a complaint;

(i) whether Suas Rov is likely to disclose the *personal information* to overseas recipients; and

(j) if Suas Rov is likely to disclose the *personal information* to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Part 3 Dealing with personal information

6 Use or disclosure of personal information

6.1 Use or disclosure

6.1.1 If Suas Rov holds *personal information* about an individual that was collected for a particular purpose (the *primary purpose*), Suas Rov will not use or disclose the information for another purpose (the *secondary purpose*) unless:

(a) the individual has consented to the use or disclosure of the information; or

(b) section 6.1.2 or 6.1.3 of Suas Rov's *Company Privacy Guidelines* applies in relation to the use or disclosure of the information.

Note 1: Section 8 of these *Company Privacy Guidelines* sets out requirements for the disclosure of *personal information* to a person who is not in Australia or an external Territory.

Note 2: In accordance with the terms of the *Health Records Act 2001*, 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, as soon as practicable, on payment of a fee not exceeding the prescribed maximum fee in Victoria, and subject to the relevant regulations, provide a copy or written summary of that *health information* to that other *health service provider*.

This obligation applies to a legal representative of a deceased *health service provider* in the same way that it applies to a *health service provider*.

6.1.2 This section of this *Company Privacy Guidelines* applies in relation to the use or disclosure of *personal information* about an individual if:

(a) the individual would reasonably expect Suas Rov to use or disclose the information for the *secondary purpose* and the *secondary purpose* is:

(i) if the information is *sensitive information*—directly related to the *primary purpose;* or

(ii) if the information is not *sensitive information*—related to the *primary purpose*; or

(b) the use or disclosure of the information is required or authorised by or under an *Australian law* or a court / tribunal order; or

(c) a *permitted general situation* exists in relation to the use or disclosure of the information by Suas Rov; or

(d) to the extent that Suas Rov is legally permitted to do so, where a *permitted health situation* exists in relation to the use or disclosure of the information by Suas Rov; or

(e) Suas Rov reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Note 1: If Suas Rov uses or discloses personal information in accordance with 6.1.2 (e), Suas Rov will make a written note of the use or disclosure.

Note 2: For the meaning of a ***permitted general situation*** and a ***permitted health situation***, see the "*Definitions"* section in section 1.2 of these Company Privacy Guidelines.

Note 3: Nothing in *HPP 2* requires Suas Rov to disclose *health information* about an individual. Suas Rov is always entitled not to disclose *health information* in the absence of a legal obligation to disclose it.

Note 4: In relation to 6.1.2 (b), an example of a relevant *Australian law* is the Victorian

Health Records Act 2001. Some specific relevant examples from that *Act* are as follows:

HPP 2.2(d) indicates that Suas Rov must not use or disclose *health information* about an individual for a *secondary purpose* unless all of the following apply—

(i) if Suas Rov, as a *health service provider*, provides 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)* of the *Health Records Act 2001* 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.

HPP 2.2(e) indicates that Suas Rov must not use or disclose *health information* about an individual for a *secondary purpose* unless all of the following apply—

(i) Suas Rov, as a *health service provider*, provides 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 Suas Rov; and

(iii) Suas Rov 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 Victorian Health Services Commissioner under *section 22* of the *Health Records Act 2001* for the purposes of this paragraph.

HPP 2.2(h) indicates that Suas Rov can disclose *health information* for a *secondary purpose* if it reasonably believes that the use or disclosure is necessary to lessen or prevent—

(i) a serious and imminent 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 Victorian Health Services Commissioner under *section 22* of the *Health Records Act 2001* for the purposes of this paragraph.

HPP 2.2(i) permits Suas Rov to disclose *health information* for a *secondary purpose* where it 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 Suas Rov, as a registered *health service provider*, would not be breaching confidence by such use or disclosure.

HPP 2.2(j) indicates that Suas Rov can disclose *health information* for a *secondary purpose* where it 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 Suas Rov is a registered *health service provider*, the use or disclosure would not be a breach of confidence.

HPP 2.4 indicates that Suas Rov, as 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 Suas Rov 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.

Note: In the *Health Records Act 2001*, an ***immediate family member*** of an individual means a person who is—

(a) a parent, child or sibling of the individual; or

(b) a spouse or domestic partner of the individual; or

(c) a member of the individual's household who is a relative of the individual; or

(d) a person nominated to a *health service provider* by the individual as a person to whom *health information* relating to the individual may be disclosed.

HPP 2.5 permits Suas Rov to 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 member of the police force, 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 Suas Rov 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 Victorian Health Services Commissioner under *section 22* for the purposes of this paragraph.

6.1.3 This section of this *Company Privacy Guidelines* applies in relation to the disclosure of personal information about an individual by Suas Rov (to the extent that Suas Rov is legally bound to do so) if:

(a) the information is biometric information or biometric templates; and

(b) the recipient of the information is an enforcement body; and

(c) the disclosure is conducted in accordance with the guidelines made by the Commonwealth Privacy Commissioner for the purposes of this paragraph.

Note: Suas Rov should review the relevant Guidelines before it releases information in this circumstance.

6.1.4 If Suas Rov has collected *personal information* about an individual where:

(a) the collection is necessary for any of the following purposes:

(i) research relevant to public health or public safety;

(ii) the compilation or analysis of statistics relevant to public health or public safety;

(iii) the management, funding or monitoring of a *health service*; and

(b) that purpose cannot be served by the collection of information about the individual that is de-identified information; and

(c) it is impracticable for Suas Rov to obtain the individual's consent to the collection; and

(d) any of the following apply:

(i) the collection is required by or under an *Australian law* (other than the *Privacy Act*);

(ii) the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind Suas Rov;

(iii) the information is collected in accordance with guidelines approved under *section 95A* of the *Privacy Act* for the purposes of subparagraph of *section 16B(2)* of the *Privacy Act*;

then Suas Rov will take such steps as are reasonable in the circumstances to ensure that the information is de-identified before Suas Rov discloses it in accordance with sections 6.1.1 or 6.1.2 of these *Company Privacy Guidelines*.

Note: Paragraphs (a) to (d) (inclusive) are drawn from *section 16B(2)* of the *Privacy Act*.

6.2 Related bodies corporate

If Suas Rov collects *personal information* from a related body corporate all of this section 6 of these *Company Privacy Guidelines* apply as if Suas Rov's *primary purpose* for the collection of the information were the *primary purpose* for which the related body corporate collected the information.

6.3 Exceptions

This section 6 of these *Company Privacy Guidelines* does not apply to the use or disclosure by Suas Rov of *personal information* for the purpose of direct marketing, nor does it relate to *government related identifiers*. These matters are subject to special provisions in these *Company Privacy Guidelines.* Please see section 7 of these *Company Privacy Guidelines* for '*direct marketing'*, and section 9 for '*government related identifiers'*.

7 Direct marketing

7.1 Direct marketing

If Suas Rov holds *personal information* about an individual, Suas Rov will not use or disclose the information for the purpose of direct marketing.

Note: Direct marketing involves the use and or the disclosure of personal information to communicate directly with an individual to promote goods and services.

Office of the Australian Information Commissioner – APP Guidelines – Draft Version - September 2013

7.2 Exceptions – personal information *other than* sensitive information

Despite section 7.1 of these *Company Privacy Guidelines*, Suas Rov may use or disclose *personal information* (other than *sensitive information*) about an individual for the purpose of direct marketing if:

(a) Suas Rov collected the information from the individual; and

(b) the individual would reasonably expect Suas Rov to use or disclose the information for that purpose; and

(c) Suas Rov provides a simple means by which the individual may easily request not to receive direct marketing communications from Suas Rov; and

(d) the individual has not made such a request to Suas Rov.

Despite section 7.1 of these *Company Privacy Guidelines*, Suas Rov may use or disclose *personal information* (other than *sensitive information*) about an individual for the purpose of direct marketing if:

(a) Suas Rov collected the information from:

  (i) the individual and the individual would not reasonably expect Suas Rov to use or disclose the information for that purpose; or

  (ii) someone other than the individual; and

(b) either:

  (i) the individual has consented to the use or disclosure of the information for that purpose; or

  (ii) it is impracticable to obtain that consent; and

(c) Suas Rov provides a simple means by which the individual may easily request not to receive direct marketing communications from Suas Rov; and

(d) in each direct marketing communication with the individual:

  (i) Suas Rov includes a prominent statement that the individual may make such a request; or

  (ii) Suas Rov otherwise draws the individual's attention to the fact that the individual may make such a request; and

(e) the individual has not made such a request to Suas Rov.

7.3 Exception – sensitive information

Despite section 7.1 of these *Company Privacy Guidelines*, Suas Rov may use or disclose *sensitive information* about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

7.4 Exception – contracted service providers

Despite section 7.1 of these *Company Privacy Guidelines*, Suas Rov may use or disclose *personal information* for the purpose of direct marketing if:

(a) Suas Rov is a contracted service provider for a Commonwealth contract; and

(b) Suas Rov collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and

(c) the use or disclosure is necessary to meet (directly or indirectly) such an obligation.

7.5 Individual may request *not* to receive direct marketing communications etc.

If Suas Rov uses or discloses *personal information* about an individual:

(a) for the purpose of direct marketing by Suas Rov; or

(b) for the purpose of facilitating direct marketing by other organisations;

the individual may:

(c) if paragraph (a) applies—request not to receive direct marketing communications from Suas Rov; and

(d) if paragraph (b) applies—request Suas Rov not to use or disclose the information for the purpose referred to in that paragraph; and

(e) request Suas Rov to provide its source of the information.

If an individual makes a request under this section 7.5, Suas Rov will not charge the individual for the making of, or to give effect to, the request and:

(a) if the request is of a kind referred to in 7.5 (c) or 7.5 (d)—Suas Rov will give effect to the request within a reasonable period after the request is made; and

(b) if the request is of a kind referred to in 7.5 (e)—Suas Rov will, within a reasonable period after the request is made, notify the individual of its source unless it is impracticable or unreasonable to do so.

Note 1: A 'reasonable period' in the case where the request is to provide the source of the information (see 7.5 (e) above), should be interpreted as being no more than 14 days unless special circumstances apply.

Office of the Australian Information Commissioner – APP Guidelines – Draft Version - September 2013

Note 2: A 'reasonable period' for a request of the kind referred to in 7.5 (c) or 7.5 (d) should also be treated as being no more than 14 days unless special circumstances apply.

7.6 Interaction with other legislation

This section 7 of these *Company Privacy Guidelines* does not apply to the extent that any of the following apply:

(a) the *Do Not Call Register Act 2006*;

(b) the *Spam Act 2003*;

(c) any Act of the Commonwealth other than the *Privacy Act*, or a Norfolk Island enactment, prescribed by the *Privacy Act regulations*.

8 Cross-border disclosure of personal information

8.1 Before a disclosure to an overseas recipient

Before Suas Rov discloses *personal information* about an individual to a person (the ***overseas recipient***):

(a) who is not in Australia or an external Territory; and

(b) who is not Suas Rov or the individual;

Suas Rov will take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the *Australian Privacy Principles* (other than *Australian Privacy Principle 1*) in relation to the information.

8.2 Exception

Section 8.1 of these *Company Privacy Guidelines* does not apply to the disclosure of *personal information* about an individual by Suas Rov to the overseas recipient if:

(a) Suas Rov reasonably believes that:

(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the *Australian Privacy Principles* protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) Suas Rov expressly informs the individual that if he or she consents to the disclosure of the information, section 8.1 of these *Company Privacy Guidelines* will not apply to the disclosure;

(ii) after being so informed, the individual consents to the disclosure; or

(c) the disclosure of the information is required or authorised by or under an *Australian law* or a court / tribunal order; or

(d) a *permitted general situation* exists in relation to the disclosure of the information by Suas Rov (other than the situations referred to in *items 4 or 5* of the table in *subsection 16A(1)* of the *Privacy Act* – that is – other than where the collection, use or disclosure is reasonably necessary for either the establishment, exercise or defence of a legal or equitable claim, or for the purposes of a confidential alternative dispute resolution process); or

(e) if Suas Rov were deemed to be an "agency" (as defined in the *Privacy Act*), and being such an agency, the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or

(f) if Suas Rov were deemed to be an "agency" as mentioned in (e) of this section, and both of the following apply:

(i) Suas Rov reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;

(ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

Note: For the meaning of a *permitted general situation*, see the "*Definition*" section in section 1.2 of these *Company Privacy Guidelines*.

8.3 Special Victorian requirements

Subject always to the provisions of sections 8.1 and 8.2 of these *Company Privacy Guidelines*, the following provisions of this section will apply:
Suas Rov may transfer *health information* about an individual to someone (other than itself or the individual) who is outside Victoria only if—

(a) Suas Rov 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 Victorian *Health Privacy Principles* or the Victorian *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 Suas Rov, 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 Suas Rov 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) Suas Rov 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 the Victorian *Information Privacy Principles* ; or
(g) the transfer is authorised or required by any other law.

9 Adoption, use or disclosure of government related identifiers and other identifiers

9.1 Adoption of government related identifiers

Suas Rov will not adopt a *government related identifier* of an individual as its own *identifier* of the individual unless:

(a) the adoption of the *government related identifier* is required or authorised by or under an *Australian law* or a court / tribunal order; or

(b) section 9.3 of these *Company Privacy Guidelines* applies in relation to the adoption.

9.2 Use or disclosure of government related identifiers

Suas Rov will not use or disclose a *government related identifier* of an individual unless:

(a) the use or disclosure of the *identifier* is reasonably necessary for Suas Rov to verify the identity of the individual for the purposes of Suas Rov's activities or functions; or

(b) the use or disclosure of the *identifier* is reasonably necessary for Suas Rov to fulfil its obligations to an agency (as defined in the *Privacy Act*) or a State or Territory authority; or

(c) the use or disclosure of the *identifier* is required or authorised by or under an *Australian law* or a court / tribunal order; or

(d) a *permitted general situation* exists in relation to the use or disclosure of the *identifier* (other than the situation referred to in *item 4 or 5* of the table in *subsection 16A(1)* – that is – other than where the collection, use or disclosure is reasonably necessary for either the establishment, exercise or defence of a legal or equitable claim, or for the purposes of a confidential alternative dispute resolution process); or

(e) Suas Rov reasonably believes that the use or disclosure of the *identifier* is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(f) section 9.3 of these *Company Privacy Guidelines* applies in relation to the use or disclosure.

Note: For the meaning of a *permitted general situation*, see the "*Definition*" section in section 1.2 of these *Company Privacy Guidelines*.

9.3 Regulations about adoption, use or disclosure

This section applies in relation to the adoption, use or disclosure by Suas Rov of a *government related identifier* of an individual if:

(a) the *identifier* is prescribed by the regulations; and

(b) Suas Rov is an organisation prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and

(c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

Note: There are prerequisites that must be satisfied before the matters mentioned in this section of these *Company Privacy Guidelines* are prescribed. In essence, *subsection*

100(2) of the *Privacy Act* provides that the Minister must be satisfied that before the Governor-General makes regulations for the purposes of *Australian Privacy Principle 9.3* that prescribe '*a government related identifier*', 'an organisation or a class of organisations', and 'the circumstances' (see (a), (b), and (c) above), the relevant Commonwealth agency or State or Territory authority has agreed that the adoption, use or disclosure of the *identifier* by the organisation, or the class of organisations, in the circumstances is appropriate, and, has consulted the Australian Information Commissioner about that adoption, use or disclosure, and, the adoption, use or disclosure of the *identifier* by the organisation, or the class of organisations, in the circumstances can only be for the benefit of the individual to whom the *identifier* relates.

9.4 Identifiers – general

Subject always to the provisions of sections 9.1, 9.2 and 9.3 of these *Company Privacy Guidelines*, the following provisions of this section will apply:

9.4.1 Suas Rov will not assign *identifiers* to individuals unless the assignment of identifiers is necessary to enable Suas Rov to carry out any of its functions efficiently.

9.4.2 Suas Rov will not adopt as its own *identifier* of an individual an *identifier* of the individual that has been assigned by another organisation unless—

(a) it is necessary to enable Suas Rov to carry out any of its functions efficiently; or

(b) Suas Rov has obtained the consent of the individual to the use of the *identifier*; or

(c) Suas Rov is an outsourcing organisation adopting the *identifier* created by a contracted service provider in the performance of its obligations to Suas Rov under a State contract.

9.4.3 Suas Rov will not use or disclose an *identifier* assigned to an individual by another organisation unless—

(a) the use or disclosure is necessary for Suas Rov to fulfil its obligations to the other organisation; or

(b) one or more of the following paragraphs applies to the use or disclosure:

- Suas Rov reasonably believes that the use or disclosure is necessary to lessen or prevent—
  - (i) a serious and imminent threat to an individual's life, health, safety or welfare; or
  - (ii) a serious threat to public health, public safety, or public welfare; or
- Suas Rov 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
- the use or disclosure is required or authorised by or under law; or
- Suas Rov 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

(c) Suas Rov has obtained the consent of the individual to the use or disclosure.

9.4.4 Suas Rov will not require an individual to provide an *identifier* in order to obtain a service unless the provision of the *identifier* is required or authorised by law or the provision is in connection with the purpose (or a directly related purpose) for which the *identifier* was assigned.

Part 4	**Integrity of personal information**
10	**Quality of personal information**
10.1	Suas Rov will take such steps (if any) as are reasonable in the circumstances to ensure that the *personal information* that it collects is accurate, up-to-date and complete. [1]
10.2	Suas Rov will take such steps (if any) as are reasonable in the circumstances to ensure that the *personal information* that it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.
11	**Security of personal information**
11.1	If Suas Rov holds *personal information*, Suas Rov will take such steps as are reasonable in the circumstances to protect the information: (a) from misuse, interference and loss; and (b) from unauthorised access, modification or disclosure.
11.2	If: (a) Suas Rov holds *personal information* about an individual; and (b) Suas Rov no longer needs the information for any purpose for which the information may be used or disclosed by it under these *Company Privacy Guidelines*; and (c) the information is not contained in a Commonwealth record; and (d) Suas Rov is not required by or under an *Australian law*, or a court / tribunal order, to retain the information; Suas Rov will take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified. Note 1: Suas Rov must consider the terms of the relevant Victorian *Health Privacy Principles* before it deletes any *health information* from its records. In particular; Suas Rov 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 *Health Records Act 2001 regulations* or any other law; or (b) the deletion is not contrary to the *Health Records Act 2001 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.

Note 2: If Suas Rov deletes *health information* in accordance with the above (*HPP 4.2), it* 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.

Note 3: If Suas Rov transfers *health information* to another individual or organisation and does not continue to hold a record of that information, it must make a written note of the name and address of the individual or organisation to whom it was transferred.

Note 4: In circumstances where Suas Rov may be an organisation that is not a *health service provider,* it 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 the *Health Records Act 2001*, the regulations made under the *Health Records Act 2001,* or any other law.

Note 5: If Suas Rov transfers, closes or amalgamates a *health service* it shall handle an individual's *health information* in the way that is prescribed in *Health Privacy Principle 10* and otherwise in accordance with the *Health Records Act 2001* and the *Privacy Act*.
Note 5: Suas Rov must consider the terms of the *Public Records Act (Victoria) 1973* before it takes any steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which information was provided.

Part 5 Access to, and correction of, personal information

APP Part 5

12 Access to personal information

12.1 Access

If Suas Rov holds *personal information* about an individual, Suas Rov will, on request by the individual, give the individual access to the information.

Note: On request by an individual, Suas Rov will take reasonable steps—

(a) to let the individual know—

(i) whether Suas Rov 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 Suas Rov 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 Suas Rov collects, holds, uses and discloses the information.

12.2 Exception to access—agency

If Suas Rov is deemed to be an "*agency*" (as defined in the *Privacy Act*), and, if Suas Rov is required or authorised to refuse to give the individual access to the *personal information* by or under:

(i) the *Freedom of Information Act*; or

(ii) any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;

then, despite section 12.1 of these *Company Privacy Guidelines*, Suas Rov is not required to give access to the extent that Suas Rov is required or authorised to refuse to give access.

A

12.3 Exception to access—Suas Rov

Suas Rov, as an organisation, and despite section 12.1, is not required to give an individual access to his or her *personal information* to the extent that:

(a) Suas Rov reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

(b) giving 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 or anticipated legal proceedings between Suas Rov and the individual, and would not be accessible by the process of discovery in those proceedings; or

(e) giving access would reveal the intentions of Suas Rov in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) giving access would be unlawful; or

(g) denying access is required or authorised by or under an *Australian law* or a court / tribunal order; or

(h) both of the following apply:

(i) Suas Rov has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to Suas Rov's functions or activities has been, is being or may be engaged in;

(ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(j) giving access would reveal evaluative information generated within Suas Rov in connection with a commercially sensitive decision-making process.

Note 1: The provisions of the *Health Records Act 2001* in *Division 3 of Part 5* provide certain conditions that Suas Rov must follow if it refuses to allow an individual to access his or her *health information* on the ground that providing access would pose a serious threat to the life or health of the individual. The opportunity exists in some circumstances for the information to be discussed with a suitably qualified health service provider (nominated by either Suas Rov or the individual) and both Suas Rov and the individual have certain rights, and certain time restrictions apply to the exercise of such rights.

Note 2: Further to section 12.3(c) above, the *Health Privacy Principles* allow access to be denied to an individual in respect to that individual's *health information* if 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, the individual has been provided with access to the health information in accordance with the relevant rules and is making an unreasonable, repeated request for access to the same information in the same way.

Note 3: The *Health Privacy Principles* allow access to be denied to an individual in respect to that individual's *health information* if the information is subject to confidentiality. See notation in section 3.1 above. *Section 27* of the *Health Records Act 2001* describes the situation where *health information* is given in confidence.

12.4 Dealing with requests for access

Suas Rov will:

(a) respond to the request for access to the *personal information* within a reasonable period after the request is made, but if Suas Rov is deemed to be an "agency" (as defined in the *Privacy Act*), then Suas Rov will respond to the request within 30 days after the request is made;

(b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Note: Suas Rov should use its best endeavors to interpret the expression '*reasonable period*' referred to in 12.4(a) as meaning a period not exceed 30 days (*Office of the Australian Information Commissioner – APP Guidelines – Draft Version - September 2013 - recommendation)* notwithstanding that the *Information Privacy Principles* provide a maximum period of 45 days.

Office of the Australian Information Commissioner-APP Guidelines- Draft Version - September 2013; IPP 6.8

12.5 Other means of access

If Suas Rov refuses:

(a) to give access to the *personal information* because of section 12.2 or 12.3 of these *Company Privacy Guidelines*; or

(b) to give access in the manner requested by the individual;

Suas Rov will take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of Suas Rov and the individual.

12.6 Access through an intermediary

Without limiting section 12.5 of these *Company Privacy Guidelines*, access may be given through the use of a mutually agreed intermediary.

12.7 Access charges

If Suas Rov is deemed to be an "*agency*" (as defined in the *Privacy Act*), Suas Rov will not charge the individual for the making of the request or for giving access to the *personal information*.

12.8 If Suas Rov, as an organisation, charges the individual for giving access to the personal information, the charge must not be excessive and must not apply to the making of the request.

Note 1: If Suas Rov charges for providing access to *personal information*, Suas Rov—

(a) will advise an individual who requests access to *personal information* that Suas Rov will provide access on the payment of the prescribed fee; and

(b) may refuse access to the *personal information* until the fee is paid.

Note 2: The *Health Records Regulations 2012* specify maximum fees applicable to the granting of access to *health information*.

See http://health.vic.gov.au/healthrecords/regs.htm#tableoffees for details.

12.9 Refusal to give access

If Suas Rov refuses to give access to the *personal information* because of sections 12.2 or 12.3 of these *Company Privacy Guidelines*, or to give access in the manner

requested by the individual, Suas Rov will give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

12.10 If Suas Rov refuses to give access to the *personal information* because of paragraph 12.3(j) of section 12.3 of these *Company Privacy Guidelines*, the reasons for the refusal may include an explanation for the commercially sensitive decision.

13 Correction of personal information

13.1 Correction

If Suas Rov holds *personal information* about an individual and Suas Rov is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, or, the individual requests Suas Rov to correct the information, Suas Rov will take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

Note 1: Suas Rov must not delete the information otherwise than in accordance with *HPP 4.2* (see also section 11.2 of these Company Privacy Guidelines).

Note 2: If Suas Rov accepts the need to correct the *health information* but—

(a) Suas Rov 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—

then, Suas Rov 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.

Note 3: If Suas Rov corrects *health information* about an individual, it must if practicable, record with the correction the name of the person who made the correction and the date on which the correction is made.

13.2 Notification of correction to third parties

If Suas Rov corrects *personal information* about an individual that Suas Rov previously disclosed to a third party, and the individual requests Suas Rov to notify the third party of the correction, Suas Rov will take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

Note: If Suas Rov corrects *health information* about an individual, it must take reasonable steps to notify any health service providers to whom Suas Rov disclosed the *health information* before its correction and who may reasonably be expected to rely on that information in the future.

13.3 Refusal to correct information

If Suas Rov refuses to correct the *personal information* as requested by the individual, Suas Rov will give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

13.4 Request to associate a statement

If:

(a) Suas Rov refuses to correct the *personal information* as requested by the individual; and

(b) the individual requests Suas Rov to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading;

then, Suas Rov will take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

13.5 Dealing with requests

If a request is made under sections 13.1 or 13.4 of these *Company Privacy Guidelines*, Suas Rov will respond to the request within a reasonable period after the request is made, but if Suas Rov is deemed to be an "*agency*" (as defined in the *Privacy Act*), then Suas Rov will respond to the request within 30 days after the request is made.

Suas Rov will not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the *personal information* (as the case may be).

Note 1: The '*reasonable period*' referred to in this section 13.5 should not (as a general guide) exceed 30 calendar days. This should be the case notwithstanding that the Victorian *Information Privacy Principles* provide a maximum period of 45 days. However, if the information is *health information,* then pursuant to the Victorian *Health Privacy Principles*, the request must be acted on as soon as practicable, but not later than 30 days.

Office of the Australian Information Commissioner-APP Guidelines- Draft Version - September 2013; HPP 6.9

Note 2: The term '*respond*' in this section 13.5 means to either correct the personal information as requested by the individual, or to notify the individual of Suas Rov's refusal to correct it.

Office of the Australian Information Commissioner-APP Guidelines- Draft Version - September 2013

SECTION 3 – Work Instructions

	Procedure steps	Responsibility
1.	**Access To Personal Information**	
	1.1 Access to Personal Information Suas Rov will provide access to personal information under: **1.1(a)** Freedom of Information legislation **1.1(b)** Legislative Obligations **1.1(c)** Individual Consent Arrangements	Staff
	1.2 Access to Personal Information – Staff **1.2(a)** Company staff will only be provided with access to personal information where it is necessary to carry out their responsibilities.	Staff
	1.3 Access to Employee Records Staff may request access to their own employee record(s) from: **1.3(a)** Manager – HR Administration, for records held by the Human Resources Department **1.3(b)** Heads of Management Units, for locally held records **1.3(c)** Staff may also apply for access to their records under the Company Freedom of Information process.	Human Resources / Head of function
2.	**Disclosure Of Personal Information**	

	2.1 The disclosure by the Company of all personal, health and sensitive information is subject to other legislative requirements (eg: the Freedom of Information Act 1982 (Vic.)) **2.2** The Company will disclose personal information to a third party on request of an individual, where it receives a written authorisation (signed) by the individual to be released for a specified purpose. **2.3** The Company will not require the written authorisation where the disclosure is authorised by law.	Staff Heads of function
3.	**Privacy Compliance**	
	3.1 All Heads of Management Units are responsible for privacy compliance in their management unit. **3.2** Head of Management Units must ensure that an appropriate Privacy Statement is in place where their Unit collects any personal information. These will be developed, where necessary, in consultation with the Compliance Officer. **3.3** THIS SECTION UNDER REVIEW: Where a Head of function is responsible for an information technology system, they are required to ensure that the applicable system complies with privacy legislation. **3.4** The Company must not acquire or implement information systems that are not privacy compliant.	Heads of function
4.	**Privacy Complaints Handling Procedure**	
	The following procedures apply if an individual considers that the Company has breached this policy or the privacy laws in respect of that individual: **4.1. Complainant to Provide Details of Complaint in Writing** A written complaint must be lodged in accordance with the Complaints, Reviews, Appeals and Feedback Policy within six (6) months of the time the complainant first became aware of the apparent breach. A complaint or request for further information can be made to the Compliance Officer – details available from; jmcmahon@suasrov.com.au The Company Counselling Service and Medical Service may require an individual to pay a fee in relation to their request to access their health information. The fee will set at the rate prescribed by the Health Records Regulations 2002. **4.2. Resolution of Complaint** The complaint is to be reviewed and managed as set out in the Complaints, Reviews, Appeals and Feedback Policy. **4.3 Consequences if this Policy is Breached**	Company Members / Members of the Public Complainant Heads of function Human Resources / Heads of function

	Subject to any overriding legal or contractual requirement, disciplinary action may be instigated against any staff member who breaches this policy, which may result in the employee being summarily dismissed in circumstances that the Company considers there to have been a serious breach.	

SUPPORTING DOCUMENTATION

Related Material

Name	Location	Document Type
Guidelines to Privacy in the Business, Health Sector [under s.95A of the Privacy Act 1988] and Government (as amended from time to time)	http://www.privacy.gov.au/health/guidelines/	Regulatory Guidelines
Guidelines to the Information Privacy Principles (as amended from time to time) (Issued by Privacy Victoria)	http://www.privacy.vic.gov.au	Regulatory Guidelines
Guidelines to the National Privacy Principles (as amended from time to time)	http://www.privacy.gov.au/act/guidelines/index.html	Regulatory Guidelines

Appendix 1 The Privacy Principles

Commonwealth Australian Privacy Principles (APPs)	Victorian *Information Privacy Principles* (IPPs)	Victorian *Health Privacy Principles* (HPPs)
APP 1 **Open and transparent management of personal information** 1.1 The object of this principle is to ensure that APP entities manage personal information in an open and transparent way. *Compliance with the Australian Privacy Principles etc.* 1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that: (a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and (b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code. *APP Privacy policy* 1.3 An APP entity must have a clearly expressed and up-to-date policy (the ***APP privacy policy***) about the management of personal information by the entity. 1.4 Without limiting subclause 1.3, the APP privacy policy of the APP entity must contain the following information: (a) the kinds of personal information that the entity collects and holds; (b) how the entity collects and holds personal information; (c) the purposes for which the entity collects, holds, uses and discloses personal information; (d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information; (e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint; (f) whether the entity is likely to disclose personal information to overseas recipients;	In these Principles— ***sensitive information*** means information or an opinion about an individual's— (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual preferences or practices; or (ix) 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 but does not include an identifier within the meaning of the **Health Records Act 2001**. **IPP 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 he or she is able to gain access to the information; and (c) the purposes for which the	**HPP 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 Services Commissioner under section 22 for the purposes of this subparagraph; (f) the collection is necessary to prevent or lessen—

(g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy. *Availability of APP privacy policy etc.* 1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available: (a) free of charge; and (b) in such form as is appropriate. Note: An APP entity will usually make its APP privacy policy available on the entity's website. 1.6 If a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form. **APP 2** **Anonymity and pseudonymity** 2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter. 2.2 Subclause 2.1 does not apply if, in relation to that matter: (a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or (b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym. **Part 2—Collection of personal information** **APP 3** **Collection of solicited personal information** *Personal information other than sensitive information* 3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities. 3.2 If an APP entity is an organisation, the entity must not collect personal	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. **IPP 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 and imminent threat to an individual's life, health, safety or welfare; or	(i) a serious and imminent 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 Services 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

information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:

(i) if the entity is an agency—the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(ii) if the entity is an organisation—the information is reasonably necessary for one or more of the entity's functions or activities; or

(b) subclause 3.4 applies in relation to the information.

3.4 This subclause applies in relation to sensitive information about an individual if:

(a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(b) a permitted general situation exists in relation to the collection of the information by the APP entity; or

(c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or

(d) the APP entity is an enforcement body and the entity reasonably believes that:

(i) if the entity is the Immigration Department—the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or

(ii) otherwise—the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(e) the APP entity is a non-profit organisation and both of the following apply:

(i) the information relates to the activities of the organisation;

(ii) the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Note: For ***permitted general situation***, see section 16A. For ***permitted health situation***, see section 16B.

Means of collection

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only

(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 Organization (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 paragraph 2.1(g), it must make a written note of the use or disclosure.

IPP 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.

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.

HPP 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

from the individual unless:

(a) if the entity is an agency:

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Solicited personal information

3.7 This principle applies to the collection of personal information that is solicited by an APP entity.

APP 4

Dealing with unsolicited personal information

4.1 If:

(a) an APP entity receives personal information; and

(b) the entity did not solicit the information;

the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.

4.2 The APP entity may use or disclose the personal information for the purposes of making the determination under subclause 4.1.

4.3 If:

(a) the APP entity determines that the entity could not have collected the personal information; and

(b) the information is not contained in a Commonwealth record;

the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

4.4 If subclause 4.3 does not apply in relation to the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had collected the information under Australian Privacy Principle 3.

APP 5

Notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

(a) to notify the individual of such matters referred to in subclause 5.2 as are

IPP 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.

IPP 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.

IPP 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 and imminent 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—

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 Services 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

reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of any such matters.

5.2 The matters for the purposes of subclause 5.1 are as follows:

(a) the identity and contact details of the APP entity;

(b) if:

(i) the APP entity collects the personal information from someone other than the individual; or

(ii) the individual may not be aware that the APP entity has collected the personal information;

the fact that the entity so collects, or has collected, the information and the circumstances of that collection;

(c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order—the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);

(d) the purposes for which the APP entity collects the personal information;

(e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;

(f) any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;

(g) that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;

(h) that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(i) whether the APP entity is likely to disclose the personal information to overseas recipients;

(j) if the APP entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Part 3—Dealing with personal information

APP 6

Use or disclosure of personal information

Use or disclosure

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction; or

(j) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(k) the protection of public revenue; or

(l) the prevention, detection, investigation or remedying of seriously improper conduct; or

(m) 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

(n) 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 paragraphs 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

(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 Services 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 Services 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 and imminent 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 Services 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 service provider, the use or disclosure would not

6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the ***primary purpose***), the entity must not use or disclose the information for another purpose (the ***secondary purpose***) unless:

(a) the individual has consented to the use or disclosure of the information; or

(b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.

6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:

(a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:

(i) if the information is sensitive information—directly related to the primary purpose; or

(ii) if the information is not sensitive information—related to the primary purpose; or

(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or

(d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or

(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Note: For ***permitted general situation***, see section 16A. For ***permitted health situation***, see section 16B.

6.3 This subclause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if:

(a) the agency is not an enforcement body; and

(b) the information is biometric information or biometric templates; and

(c) the recipient of the information is an enforcement body; and

(d) the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.

6.4 If:

(a) the APP entity is an organisation; and

(b) subsection 16B(2) applied in relation to the collection of the personal information by the entity;

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.

IPP 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 paragraphs 2.1(d) to 2.1(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.

IPP 8

Anonymity

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 service provider, 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

the entity must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the entity discloses it in accordance with subclause 6.1 or 6.2.

Written note of use or disclosure

6.5 If an APP entity uses or discloses personal information in accordance with paragraph 6.2(e), the entity must make a written note of the use or disclosure.

Related bodies corporate

6.6 If:

(a) an APP entity is a body corporate; and

(b) the entity collects personal information from a related body corporate;

this principle applies as if the entity's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Exceptions

6.7 This principle does not apply to the use or disclosure by an organisation of:

(a) personal information for the purpose of direct marketing; or

(b) government related identifiers.

APP 7

Direct marketing

Direct marketing

7.1 If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Exceptions—personal information other than sensitive information

7.2 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from the individual; and

(b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) the individual has not made such a request to the organisation.

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

IPP 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 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 Information Privacy Principles.

IPP 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 under law; or

(c) the collection is necessary to prevent or lessen a serious and imminent 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

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 member of the police force, 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 Services Commissioner under section 22 for the purposes of this paragraph.

HPP 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.

HPP 4

Data Security and Data Retention

4.1 An organisation must take reasonable

7.3 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if: (a) the organisation collected the information from: (i) the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or (ii) someone other than the individual; and (b) either: (i) the individual has consented to the use or disclosure of the information for that purpose; or (ii) it is impracticable to obtain that consent; and (c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and (d) in each direct marketing communication with the individual: (i) the organisation includes a prominent statement that the individual may make such a request; or (ii) the organisation otherwise draws the individual's attention to the fact that the individual may make such a request; and (e) the individual has not made such a request to the organisation. *Exception—sensitive information* 7.4 Despite subclause 7.1, an organisation may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose. *Exception—contracted service providers* 7.5 Despite subclause 7.1, an organisation may use or disclose personal information for the purpose of direct marketing if: (a) the organisation is a contracted service provider for a Commonwealth contract; and (b) the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and (c) the use or disclosure is necessary to meet (directly or indirectly) such an obligation. *Individual may request not to receive direct marketing communications etc.* 7.6 If an organisation (the ***first organisation***) uses or discloses personal information about an individual: (a) for the purpose of direct marketing by the first organisation; or (b) for the purpose of facilitating direct	(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.	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. **HPP 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—

marketing by other organisations; the individual may: (c) if paragraph (a) applies—request not to receive direct marketing communications from the first organisation; and (d) if paragraph (b) applies—request the organisation not to use or disclose the information for the purpose referred to in that paragraph; and (e) request the first organisation to provide its source of the information. 7.7 If an individual makes a request under subclause 7.6, the first organisation must not charge the individual for the making of, or to give effect to, the request and: (a) if the request is of a kind referred to in paragraph 7.6(c) or (d)—the first organisation must give effect to the request within a reasonable period after the request is made; and (b) if the request is of a kind referred to in paragraph 7.6(e)—the organisation must, within a reasonable period after the request is made, notify the individual of its source unless it is impracticable or unreasonable to do so. *Interaction with other legislation* 7.8 This principle does not apply to the extent that any of the following apply: (a) the *Do Not Call Register Act 2006*; (b) the *Spam Act 2003*; (c) any other Act of the Commonwealth, or a Norfolk Island enactment, prescribed by the regulations. **APP 8** **Cross-border disclosure of personal information** 8.1 Before an APP entity discloses personal information about an individual to a person (the ***overseas recipient***): (a) who is not in Australia or an external Territory; and (b) who is not the entity or the individual; the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information. Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles. 8.2 Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if: (a) the entity reasonably believes that:		(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. **HPP 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 Services 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 Services 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 (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

(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and (ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or (b) both of the following apply: (i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure; (ii) after being so informed, the individual consents to the disclosure; or (c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or (d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or (e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or (f) the entity is an agency and both of the following apply: (i) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; (ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body. Note: For ***permitted general situation***, see section 16A. **APP 9** **Adoption, use or disclosure of government related identifiers** *Adoption of government related identifiers* 9.1 An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless: (a) the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or (b) subclause 9.3 applies in relation to the adoption. Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A. *Use or disclosure of government related*		(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

identifiers 9.2 An organisation must not use or disclose a government related identifier of an individual unless: (a) the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions; or (b) the use or disclosure of the identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or (c) the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or (d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier; or (e) the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or (f) subclause 9.3 applies in relation to the use or disclosure. Note 1: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A. Note 2: For ***permitted general situation***, see section 16A. *Regulations about adoption, use or disclosure* 9.3 This subclause applies in relation to the adoption, use or disclosure by an organisation of a government related identifier of an individual if: (a) the identifier is prescribed by the regulations; and (b) the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and (c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations. Note: There are prerequisites that must be satisfied before the matters mentioned in this subclause are prescribed, see subsections 100(2) and (3). **Part 4—Integrity of personal information** **APP 10** **Quality of personal information**		(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.

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete. 10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant. **APP 11** **Security of personal information** 11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information: (a) from misuse, interference and loss; and (b) from unauthorised access, modification or disclosure. 11.2 If: (a) an APP entity holds personal information about an individual; and (b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and (c) the information is not contained in a Commonwealth record; and (d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information; the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified. **Part 5—Access to, and correction of, personal information** **APP 12** **Access to personal information** *Access* 12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information. *Exception to access—agency* 12.2 If: (a) the APP entity is an agency; and (b) the entity is required or authorised to refuse to give the individual access to the		**HPP 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. **HPP 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.

personal information by or under: (i) the Freedom of Information Act; or (ii) any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents; then, despite subclause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access. *Exception to access—organisation* 12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that: (a) the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or (b) giving 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 or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or (e) giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or (f) giving access would be unlawful; or (g) denying access is required or authorised by or under an Australian law or a court/tribunal order; or (h) both of the following apply: (i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in; (ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or (i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or (j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process. *Dealing with requests for access* 12.4 The APP entity must: (a) respond to the request for access to the personal information: (i) if the entity is an agency—within 30 days after the request is made; or (ii) if the entity is an organisation—within a reasonable period after the request is made; and (b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.		**HPP 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. **HPP 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.

Other means of access 12.5 If the APP entity refuses: (a) to give access to the personal information because of subclause 12.2 or 12.3; or (b) to give access in the manner requested by the individual; the entity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual. 12.6 Without limiting subclause 12.5, access may be given through the use of a mutually agreed intermediary. *Access charges* 12.7 If the APP entity is an agency, the entity must not charge the individual for the making of the request or for giving access to the personal information. 12.8 If: (a) the APP entity is an organisation; and (b) the entity charges the individual for giving access to the personal information; the charge must not be excessive and must not apply to the making of the request. *Refusal to give access* 12.9 If the APP entity refuses to give access to the personal information because of subclause 12.2 or 12.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out: (a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and (b) the mechanisms available to complain about the refusal; and (c) any other matter prescribed by the regulations. 12.10 If the APP entity refuses to give access to the personal information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision. **APP 13** **Correction of personal information** *Correction* 13.1 If: (a) an APP entity holds personal information about an individual; and (b) either: (i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is		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 Services 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—

inaccurate, out-of-date, incomplete, irrelevant or misleading; or (ii) the individual requests the entity to correct the information; the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading. *Notification of correction to third parties* 13.2 If: (a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and (b) the individual requests the entity to notify the other APP entity of the correction; the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so. *Refusal to correct information* 13.3 If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out: (a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and (b) the mechanisms available to complain about the refusal; and (c) any other matter prescribed by the regulations. *Request to associate a statement* 13.4 If: (a) the APP entity refuses to correct the personal information as requested by the individual; and (b) the individual requests the entity to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading; the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information. *Dealing with requests* 13.5 If a request is made under subclause 13.1 or 13.4, the APP entity: (a) must respond to the request: (i) if the entity is an agency—within 30 days after the request is made; or (ii) if the entity is an organisation—within a reasonable period after the request is made; and (b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal		(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. **HPP 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.

information (as the case may be).		