

PRIVACY POLICY

Elan Vital Inc ARBN 007 505 535 ('EV') and Ivory's Rock Conference Centre Pty Ltd ACN 068 618 922 ('IRCC')

1.0 INTRODUCTION

- 1.1. IRCC is responsible for the management of Ivory's Rock Conference Centre on behalf of EV including the collection of personal information.
- 1.2. EV/IRCC ('we' or 'us' meaning either or both of us) are sensitive to concerns that you may have regarding the use, disclosure and/or security of personal information collected by us. We are both bound by the *National Privacy Principles* (NPPs) and committed to your privacy. Our joint policy on the management of personal information is set out below as our joint privacy policy ('the policy'). Definitions to key terms are set out in Appendix 1 and the NPPs are attached as Appendix 2.

2.0 EMPLOYEE RECORDS EXEMPTION

- 2.1. The policy does not apply to employee records. Under section 7B (3) of the *Privacy Act 1988* (Cth) ('the Act'), acts done or practices engaged in by us regarding current or former individuals employed by us are exempt from the operation of the Act including the NPPs if the act or practice directly related to:
 - 2.1.1 a current or former employment relationship between us and the individual; and
 - 2.1.2 an employee record held by us and relating to the individual.
- 2.2 In the absence of legal authority to the contrary, we will ordinarily regard this exemption as not applying to volunteer records.

3.0 COLLECTION OF PERSONAL INFORMATION

- 3.1. We will ordinarily collect personal information where the information is necessary for our functions or activities including:
 - 3.1.1 registration for conferences, functions and events;
 - 3.1.2 your involvement as a volunteer;
 - 3.1.3 administration of loans and contributions;
 - 3.1.4 sales and subscriptions of materials and services; and
 - 3.1.5 registration of your interest in being informed of upcoming events and activities.
- 3.2. If we collect personal information we will take reasonable steps to ensure that you are aware:

- 3.2.1 that the information is being collected;
 - 3.2.2 of the purposes of collection;
 - 3.2.3 that you can access the information;
 - 3.2.4 of the types of organisations (if any) to which we may disclose the information;
 - 3.2.5 of any law that requires the information to be collected; and
 - 3.2.6 of the main consequences (if any) for you if all or part of the information is not provided.
- 3.3. Wherever it is reasonable and practicable to do so, we will collect information about you only from you.

4.0 USE AND DISCLOSURE OF PERSONAL INFORMATION

- 4.1. We will not use or disclose personal information about an individual for a purpose other than the primary purpose of collection otherwise than in accordance with the NPPs and in particular, NPP 2.
- 4.2. As permitted by NPP 2.1, however:
- 4.2.1 IRCC will from time to time disclose personal information to EV to facilitate functions and activities including those set out in paragraph 3.1.
 - 4.2.2 EV will from time to time disclose personal information to IRCC to assist in the coordination and management of functions and activities including those set out in paragraph 3.1.
- 4.3. We will obtain your consent to use or disclose personal information where such use or disclosure is not otherwise permitted by NPP 2. This means that it is not unlikely that we will obtain your consent before using or disclosing sensitive information about you, including your health information.

5.0 DATA QUALITY

- 5.1. We will take reasonable steps to make sure that the personal information that we collect, use or disclose is accurate, complete and up-to-date.

6.0 DATA SECURITY

- 6.1. We will take reasonable steps to:
- 6.1.1 protect the personal information that we hold from misuse and loss, and from unauthorised access, modification or disclosure.
 - 6.1.2 destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under NPP 2.

7.0 OPENNESS

- 7.1. At your request, we will take reasonable steps to let you know, generally, what sort of personal information we hold, for what purposes, and how we collect, store, use and disclose that information.

8.0 ACCESS AND CORRECTION

- 8.1. If we hold personal information about you, you may access that information on request, except where:
- 8.1.1 in the case of personal information other than health information - providing access would pose a serious and imminent threat to the life or health of any individual; or
 - 8.1.2 providing access would have an unreasonable impact upon the privacy of other individuals; or
 - 8.1.3 the request for access is frivolous or vexatious; or
 - 8.1.4 the information relates to existing or anticipated legal proceedings between us and you, and the information would not be accessible by the process of discovery in those proceedings; or
 - 8.1.5 providing access would reveal our intentions in relation to negotiations with you in such a way as to prejudice those negotiations; or
 - 8.1.6 providing access would be unlawful; or
 - 8.1.7 denying access is required or authorised by or under law; or
 - 8.1.8 providing access would be likely to prejudice an investigation of possible unlawful activity; or
 - 8.1.9 providing access would be likely to prejudice:
 - (a) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or
 - (b) the enforcement of laws relating to the confiscation of the proceeds of crime; or
 - (c) the protection of public revenue; or
 - (d) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
 - (e) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;by or on behalf of an enforcement body; or
 - 8.1.10 an enforcement body performing a lawful security function asks us not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

- 8.2 If providing access would reveal information generated by us in connection with a commercially sensitive decision-making process, we may give you an explanation for the commercially sensitive decision rather than direct access to the information.
- 8.3 We may levy a reasonable charge for providing access to personal information, however any such charge will not apply to lodging a request for access to personal information.
- 8.4 If we hold personal information about an individual that is not accurate, complete and up-to-date, we will take reasonable steps to correct such information.
- 8.5 We will provide reasons for any denial of access to, or refusal to correct any personal information.

9.0 IDENTIFIERS

- 9.1. We will not adopt as our own identifier of an individual, an identifier of an individual that has been assigned by a government agency or other precluded entity under NPP 7.
- 9.2. We will not use or disclose an identifier assigned to an individual by a government agency or other precluded entity under NPP 7 unless:
 - 9.2.1 the use or disclosure is necessary for us to fulfil our obligations to the agency; or
 - 9.2.2 one or more paragraphs 2.1(e) to 2.1(h) (inclusive) of NPP 2 apply to the use or disclosure; or
 - 9.2.3 the use or disclosure is otherwise permitted under NPP 7.

10.0 ANONYMITY

- 10.1. Wherever it is lawful and practicable, individuals have the option of not identifying themselves when entering into transactions with us.

11.0 TRANSBORDER DATA FLOWS

- 11.1. We may transfer personal information to someone who is in a foreign country only if:
 - 11.1.1 we reasonably believe that the recipient 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 NPPs; or
 - 11.1.2 the individual consents to the transfer; or
 - 11.1.3 the transfer is necessary for the performance of a contract between the individual and us, or for the implementation of pre-contractual measures taken in response to the individual's request; or

- 11.1.4 the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between us and a third party; or
- 11.1.5 all of the following apply:
 - (a) the transfer is for the benefit of the individual;
 - (b) it is impracticable to obtain the consent of the individual to that transfer;
 - (c) if it were practicable to obtain such consent, the individual would be likely to give it; or
- 11.1.6 We have taken reasonable steps to ensure that the information which we have transferred will not be held, used or disclosed by the recipient of the information inconsistently with the NPPs.

12.0 SENSITIVE INFORMATION

- 12.1. We will not collect sensitive information about an individual unless:
 - 12.1.1 the individual has consented; or
 - 12.1.2 the collection is required by law; or
 - 12.1.3 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:
 - (a) is physically or legally incapable of giving consent to the collection; or
 - (b) physically cannot communicate consent to the collection; or
 - (c) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.
- 12.2. We will collect health information about an individual:
 - 12.2.1 only with the consent of that individual; and
 - 12.2.2 otherwise only in accordance with the NPPs.

13.0 CONTACT DETAILS

- 13.1 We are happy to provide you with further information on the way we manage the personal information that we hold. To obtain such further information or other assistance or notify us of a privacy concern or breach of privacy, please contact our privacy officer Stuart Hogarth at:

PO Box 521 Toowong, QLD 4066 AUSTRALIA

Ph: +61-7-5464 8331

Fax: +61-7-5464 8314

Email: elan@gil.com.au

APPENDIX 1

1. Definitions

1.1 **Employee record**, in relation to an employee, means a record of personal information relating to the employment of the employee. Examples of personal information relating to the employment of the employee are health information about the employee and personal information about all or any of the following:

- (a) the engagement, training, disciplining or resignation of the employee;
- (b) the termination of the employment of the employee;
- (c) the terms and conditions of employment of the employee;
- (d) the employee's personal and emergency contact details;
- (e) the employee's performance or conduct;
- (f) the employee's hours of employment;
- (g) the employee's salary or wages;
- (h) the employee's membership of a professional or trade association;
- (i) the employee's trade union membership;
- (j) the employee's recreation, long service, sick, personal, maternity, paternity or other leave;
- (k) the employee's taxation, banking or superannuation affairs.

1.2 **Enforcement body** means:

- (a) the Australian Federal Police; or
- (b) the ACC; or
- (c) the Australian Customs Service; or
- (d) the Australian Prudential Regulation Authority; or
- (e) the Australian Securities and Investments Commission; or
- (f) another agency, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law; or
- (g) another agency, to the extent that it is responsible for administering a law relating to the protection of the public revenue; or
- (h) a police force or service of a State or a Territory; or
- (i) the New South Wales Crime Commission; or
- (j) the Independent Commission Against Corruption of New South Wales; or
- (k) the Police Integrity Commission of New South Wales; or
- (l) the Criminal Justice Commission of Queensland; or
- (m) another prescribed authority or body that is established under a law of a State or Territory to conduct criminal investigations or inquiries; or
- (n) a State or Territory authority, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law; or
- (o) a State or Territory authority, to the extent that it is responsible for administering a law relating to the protection of the public revenue.

1.3 **Health information** means:

- (a) information or an opinion about:
 - (i) the health or a disability (at any time) of an individual; or
 - (ii) an individual's expressed wishes about the future provision of health services to him or her; or
 - (iii) a health service provided, or to be provided, to an individual; that is also personal information; 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.

1.4 **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 person performing it:
 - (i) to assess, record, maintain or improve the individual's health; or
 - (ii) to diagnose the individual's illness or disability; or
 - (iii) to treat the individual's illness or disability or suspected illness or disability; or
- (b) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

1.5 **Personal information** means information or an opinion (including information or an opinion forming part of a database) whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Note 1: Personal information relates to a natural living person. A natural person is a human being rather than, for example, a company, which may in some circumstances, be recognised as a legal 'person' under the law.

1.6 **Record** means:

- (a) a document; or
 - (b) a database (however kept); or
 - (c) a photograph or other pictorial representation of a person;
- but does not include:
- (d) a generally available publication; or
 - (e) anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition; or
 - (f) 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
 - (fa) records (as defined in the *Archives Act 1983*) in the custody of the Archives (as defined in that Act) 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
 - (g) 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
 - (h) letters or other articles in the course of transmission by post.

1.7 **Sensitive information** means information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade union, sexual preferences or practices, criminal record or health information about an individual.

Note 2: Sensitive information is a subset of personal information.

Appendix 2

National Privacy Principles

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 information is collected; and
 - (d) the organisations (or the types of 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 subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2 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 information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:
 - (i) it is impracticable for the organisation to seek the individual's consent before that particular use; and
 - (ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and
 - (iii) the individual has not made a request to the organisation not to receive direct marketing communications; and
 - (iv) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and
 - (v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic

- means, a number or address at which the organisation can be directly contacted electronically; or
- (d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:
 - (i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and
 - (ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and
 - (iii) in the case of disclosure—the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or
 - (e) 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 or safety; or
 - (ii) a serious threat to public health or public safety; or
 - (f) 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
 - (g) the use or disclosure is required or authorised by or under law; or
 - (h) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:
 - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
 - (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 or prescribed conduct;
 - (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: It is not intended to deter organisations from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

- 2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.
- 2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.
- 2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:
 - (a) the individual:
 - (i) is physically or legally incapable of giving consent to the disclosure; or
 - (ii) physically cannot communicate consent to the disclosure; and
 - (b) a natural person (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

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

2.5 For the purposes of subclause 2.4, a person is **responsible** for an individual if the person is:

- (a) a parent of the individual; or
- (b) a child or sibling of the individual and at least 18 years old; or
- (c) a spouse or de facto spouse of the individual; or
- (d) a relative of the individual, at least 18 years old and a member of the individual's household; or
- (e) a guardian of the individual; or
- (f) 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.

2.6 In subclause 2.5:

child of an individual includes an adopted child, a step-child and a foster-child, of the individual.

parent of an individual includes a step-parent, adoptive parent and a foster-parent, of the individual.

relative of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.

sibling of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.

3 Data quality

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

4 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 for which the information may be used or disclosed under National Privacy Principle 2.

5 Openness

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

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

6 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) in the case of personal information other than health information—providing access would pose a serious and imminent threat to the life or health of any individual; or
- (b) in the case of health information—providing access would pose a serious threat to the life or health of any individual; or
- (c) providing access would have an unreasonable impact upon the privacy of other individuals; or
- (d) the request for access is frivolous or vexatious; or
- (e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or
- (f) 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
- (g) providing access would be unlawful; or
- (h) denying access is required or authorised by or under law; or
- (i) providing access would be likely to prejudice an investigation of possible unlawful activity; or
- (j) providing access would be likely to prejudice:
 - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or
 - (ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or
 - (iii) the protection of the public revenue; or
 - (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
 - (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders; by or on behalf of an enforcement body; or
 - (k) an enforcement body 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.

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

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 (k) (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, those charges:

- (a) must not be excessive; and
- (b) must not apply to lodging a request for access.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up-to-date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to do so.

6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

7 Identifiers

- 7.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:
- (a) an agency; or
 - (b) an agent of an agency acting in its capacity as agent; or
 - (c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

- 7.1A However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2).

- 7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:
- (a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or
 - (b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or
 - (c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsections 100(2) and (3).

- 7.3 In this clause:

identifier includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the *A New Tax System (Australian Business Number) Act 1999*) is not an **identifier**.

8 Anonymity

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

9 Transborder data flows

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country 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 National Privacy Principles; or
- (b) the individual consents to the transfer; or
- (c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or
- (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or
- (e) all of the following apply:
 - (i) the transfer is for the benefit of the individual;
 - (ii) it is impracticable to obtain the consent of the individual to that transfer;
 - (iii) if it were practicable to obtain such consent, the individual would be likely to give it; or
- (f) the 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 National Privacy Principles.

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 by 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
 - (ii) physically cannot communicate consent to the collection; or
 - (d) if the information is collected in the course of the activities of a non-profit organisation—the following conditions are satisfied:
 - (i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;
 - (ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or
 - (e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.
- 10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:
- (a) the information is necessary to provide a health service to the individual; and
 - (b) the information is collected:
 - (i) as required by law (other than this Act); or
 - (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.
- 10.3 Despite subclause 10.1, an organisation may collect 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 that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and
 - (c) it is impracticable for the organisation to seek the individual's consent to the collection; and
 - (d) the information is collected:
 - (i) as required by law (other than this Act); or
 - (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or
 - (iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.
- 10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.
- 10.5 In this clause:

non-profit organisation means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.