

Policy: Privacy and Security of Information

Table of Contents

Purpose	3
Scope.....	3
Policy statement	4
Opt out.....	4
Right of access.....	4
Accuracy	4
Security	5
Employment records.....	5
Contact details	5
Appendix 1: Privacy Act 1988: Schedule 3—National Privacy Principles.....	7

Purpose

The Institute of Internal Auditors-Australia (IIA-Australia) has created this Privacy Policy and Disclosure Statement (together referred to as ‘this Privacy Policy’) in order to demonstrate its firm commitment to comply with relevant privacy regulations and the foreshadowed regulatory changes.

The IIA-Australia is bound by the National Privacy Principles.

The IIA-Australia reserves the right to modify this Privacy Policy at any time. If it is changed, the changes will be posted on IIA-Australia website so that you are always aware of the sort of information collected, how the information may be used, and under what circumstances it may be disclosed by the IIA-Australia.

If at any time the IIA-Australia is required by law to release information about you or your organisation, the IIA-Australia must cooperate fully.

Scope

The Institute of Internal Auditors-Australia will only use your information together with other information for:

- ❖ member services
- ❖ recording your dealings with us
- ❖ providing advice
- ❖ processing your orders and requests
- ❖ assessing application forms and verifying information you provide (if appropriate)
- ❖ provide services to candidates and to people enquiring about study at IIA-Australia
- ❖ maintain appropriate academic and financial records
- ❖ perform other internal administrative functions
- ❖ maintain contact with past candidates and members
- ❖ provide statistical and other information required by government
- ❖ marketing.

We do not collect sensitive information if the individual has not consented to its collection (unless we are required or permitted to do so by law).

Policy statement

Disclosure of personal information

We do not disclose personal information to third parties without the owner's consent, unless required or permitted by law.

We may share your information with the Institute of Internal Auditors Inc. in the USA, in order to allow you password-protected access to its website.

We will not pass on your information to other organisations, but may contact you by mail on their behalf. We may contact you by mail, telephone, fax or email to let you know about any special offers or promotions which may be of interest to you.

It may sometimes be necessary for IIA-Australia to provide personal information to others with whom it conducts business; for example professional advisers (auditors, lawyers), insurers, and printers.

Personal information may be disclosed for the prevention, detection or investigation of criminal or proscribed conduct, or in certain circumstances in the interest of public health or public safety.

When you give us information about another person, you confirm that they have appointed you to act for them, to consent to the processing of their personal data, including sensitive personal data, to the transfer of their information abroad and to receive on their behalf any fair collection notices.

Opt out

You have the right to opt out of receiving information from the IIA-Australia; if this is the case please email enquiry@iia.org.au.

Right of access

You have the right to access your personal information (subject to some exceptions allowed by law), and to have it corrected if necessary. Please contact IIA-Australia for any changes you require. Contact details are available at the end of this Policy Document.

Accuracy

IIA-Australia takes reasonable precautions to ensure that the personal information we collect is accurate, complete and up-to-date. It is important that members and candidates keep us up-to-date with changes to their personal information, such as name and contact details.

Security

IIA-Australia takes reasonable steps to protect personal information from unauthorised access, modification or disclosure.

The IIA-Australia has security measures designed to protect against the loss, misuse and/or alteration of the information under its control. These security measures include:

- ❖ firewalls—to prevent the unauthorised access to data
- ❖ clauses in employee agreements requiring confidentiality and training on the importance of the Privacy Legislation
- ❖ appropriate security access to IIA-Australia premises
- ❖ the use of passwords for access to database information and the use of security levels within the database to ensure that staff only access the information required to perform their duties
- ❖ security bins for the disposal of written information.

The IIA-Australia aims to provide all of our website users with a safe online experience. Our system encodes your credit card and contact details to ensure its safe transfer to us.

Employment records

The employment records of employees of IIA-Australia are held by the CEO and are not subject to the provisions of the Privacy Act.

Contact details

If you have any questions relating to information we hold about you, please contact:

Executive Officer
The Institute of Internal Auditors-Australia
PO Box A2311
Sydney South NSW 1235

Telephone: **+ 61 2 9267 9155**
Facsimile: **+ 61 2 9264 9240**
E-mail: governance@iia.org.au
Website: **www.iia.org.au**

Level 7/133 Castlereagh Street
Sydney NSW 2000 Australia

The Institute of Internal Auditors-Australia

PO Box A2311
Sydney South NSW 1235

Telephone: **+ 61 2 9267 9155**
Facsimile: **+ 61 2 9264 9240**
E-mail: governance@iia.org.au
Website: **www.iia.org.au**

Level 7
133 Castlereagh Street
Sydney NSW 2000 Australia

© Copyright IIA-Australia 2011
ABN 80 001 797 557

Appendix 1: Privacy Act 1988: Schedule 3—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
- (ea) if the information is genetic information and the organisation has obtained the genetic information in the course of providing a health service to the individual:
- (i) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat is imminent) of an individual who is a genetic relative of the individual to whom the genetic information relates; and
 - (ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95AA for the purposes of this subparagraph; and
 - (iii) in the case of disclosure—the recipient of the genetic information is a genetic relative of the individual; 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 partner 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: without limiting who is a child of an individual for the purposes of this clause, each of the following is the **child** of an individual:

- (a) an adopted child, stepchild, exnuptial child or foster child of the individual; and
- (b) someone who is a child of the individual within the meaning of the Family Law Act 1975.

de facto partner has the meaning given by the Acts Interpretation Act 1901.

parent: without limiting who is a parent of an individual for the purposes of this clause, someone is the parent of an individual if the individual is his or her child because of the definition of child in this subclause.

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.

stepchild: without limiting who is a stepchild of an individual for the purposes of this clause, someone is the 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.

- 2.7 For the purposes of the definition of relative in subclause 2.6, relationships to an 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 that subclause.
- 2.8 For the purposes of the definition of sibling in subclause 2.6, an individual is also a sibling of another individual if a relationship referred to in that definition can be traced through a parent of either or both of them.

3 *Data quality*

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.