Department of Health

Contact Centre CRM Solution

Privacy Impact Assessment

June 2019

HWL EBSWORTH
LAWYERS

Table of Contents

Executive Summary **3**

1. Contact Centre CRM Solution: PIA Overview **3**

2. Summary of Findings **3**

3. Recommendations **3**

4. PIA Methodology **4**

5. Background **5**

6. Assumptions **10**

7. Community expectations **10**

8. Privacy impacts **11**

s47E(d)

s 42

Glossary **26**

s47E(d)

Schedule 2 (Australian Privacy Principles)

Executive Summary

1. Contact Centre CRM Solution: PIA Overview

1.1 The Department of Health (**Department**) is implementing the s47E(d) s47E(d) Project implements a Customer Relationship Management (**CRM**) Solution for the Department's existing Contact Centre (**Solution**). The Solution will change the way in which enquiries are currently captured and escalated by the Contact Centre, and how information collected by the Contact Centre is handled and stored by the Department.

1.2 This Privacy Impact Assessment (**PIA**) Report:

(a) assesses any risks to individual privacy presented by the implementation of the Solution as described in the Project Description;

(b) considers compliance with the *Privacy Act 1988* (Cth) (**Privacy Act**), including the Australian Privacy Principles (**APPs**);

(c) seeks to inform stakeholders about the Solution, and illustrate the focus being given by the Department to identifying and mitigating privacy risks;

(d) sets out the information lifecycle which helps to highlight any privacy risks and areas for improvement in terms of risk mitigation; and

(e) considers any safeguards that the Department will have in place to secure personal information from loss or unauthorised access, modification or disclosure.

1.3 This PIA Report has been developed in accordance with the Office of the Australian Information Commissioner (**OAIC**) Guide to Undertaking a Privacy Impact Assessment.

2. Summary of Findings

s 42

2.2 HWL Ebsworth has undertaken this PIA in consultation with the Department. HWL Ebsworth has relied on the Department for the description of the Solution contained in the Project Description, and has drafted this PIA Report on the assumption that the Project Description accurately reflects the proposed handling of personal information.

s 42

4. PIA Methodology

4.1 This PIA has been undertaken in accordance with the ten step process for undertaking a PIA recommended by the OAIC in its Guide to Undertaking a Privacy Impact Assessment.

Project Description

5. Background

5.1 The Department has general responsibility for matters including public health, primary health care, pharmaceutical benefits, regulation of therapeutic goods and health provider compliance.[1]

5.2 The Department operates an onsite Contact Centre which serves as a first point of contact for members of the public and departmental staff with enquiries about the Department's functions and activities. The Contact Centre supports the Department's strategic priorities by providing information about health programs administered by the Department.

s47E(d)

5.5 The Contact Centre can be reached by telephone, email or online enquiry form.

s47E(d)

[1] See Part 9 of the *Administrative Arrangements Order*.

s47E(d)

s47E(d)

5.19 When an enquiry comes into the Contact Centre (regardless of the channel) a record of the enquiry will be created and the following information will be collected and stored by the Solution:

[4] Australian Government, 'Legal Request Form - Privacy Impact Assessment' (Department of Health, 2018) 3.
[5] Ibid.
[6] Ibid.

(a) a Unique ID;

(b) the incoming Line/Inbox;

(c) Enquirer details (name, email, phone, address) or anonymous; and

(d) Enquiry Sensitivity Rating (the **Enquiry Details**).

s47E(d)

5.22 Contact Centre operators will create an **Issue Record** in the Solution, containing the following details about the issue(s) raised by each enquiry:

(a) Issue Type;

(b) Issue Text;

(c) Issue Outcome; and

(d) Enquirer details (name, email, phone, address) or anonymous.

s47E(d)

s47E(d)

Analysis

6. Assumptions

6.1 This PIA Report is drafted on the assumptions that:

(a) the Department's current information handling practices in relation to the operation of the Contact Centre are compliant with the Department's privacy obligations;

(b) the description of the Solution contained in the Project Description accurately reflects the proposed handling of personal information;

(c) the Department's agreement with Data#3 complies with the Privacy Act (including section 95B of that Act); and

(d) the security measures implemented by the Department in relation to the Solution in respect of personal information are compliant with APP 11.

7. Community expectations

7.1 One of the matters which must be taken into account when conducting a PIA is how consistent the project is with community values about privacy. To assess this question, APP entities can conduct consultations, review community responses to similar projects, or consider research into community attitudes about privacy.

7.2 The Department has not conducted any specific consultation with members of the community to assess their views regarding the proposed handling of personal information in connection with the Solution. Accordingly, it is appropriate to consider research into community attitudes more generally.

7.3 The OAIC commissioned the *Australian Community Attitudes to Privacy Survey 2017*, which assists in understanding contemporary community expectations regarding the management of personal information. The following findings are of relevance to this project:

(a) Australians believe that the biggest privacy risks facing the community are online services, including social media sites (32%), ID fraud and theft (19%), data security breaches (17%), risks to financial data (12%), and personal details being too easily available/ accessible/ not secure (7%);

(b) 83% of respondents to the survey believe that privacy risks are greater when dealing with an organisation online compared with other means;

(c) the pieces of information Australians are most reluctant to provide are financial details (42%), address (24%), date of birth (14%), phone numbers (13%), name (10%) and email address (5%). These figures are similar to those obtained when the OAIC last conducted the survey in 2013;

(d) when the community was asked how trustworthy they considered different types of organisation to be, the highest levels of trust were recorded for health service providers (79%), financial institutions (59%) and state and federal government departments (58%); and

(e) only 16% would avoid dealing with a government agency because of privacy concerns, compared with 58% who would avoid dealing with a private company.

7.4 Given that survey respondents believed that privacy risks are greater when dealing with an organisation online compared with other means, it is relevant that the Solution will not change the fact that individuals have a choice of the means by which they engage with the Contact

Centre (ie, telephone or online channels). That is a privacy positive feature of the ongoing operation of the Contact Centre.

7.5 Survey respondents advised that names and contact details are among the pieces of information that they are most reluctant to provide. Individuals external to the Department will be able to remain anonymous when dealing with the Contact Centre by telephone. The implementation of the Solution will not change the Department's current practice of collecting contact details from individuals external to the Department only in order to escalate the enquiry within the Department. s 42

7.6 Seventeen per cent of survey respondents considered that data security breaches presented the biggest privacy risk. It is probable (although difficult to assess) that the community would be reassured by a description of the security features of the Solution s47E(d) s47E(d) s47E(d) noting that the survey respondents indicated a relatively high level of trust in the information handling practices of federal government departments.

7.7 In the absence of specific consultation with the community, it is difficult to gauge precisely how the community may respond to the proposed handling of personal information in connection with the Solution. However, in light of the research conducted by the OAIC and the discussion above, this PIA finds that it is likely that the implementation of the Solution will be consistent with community values about privacy.

8. Privacy impacts

8.1 In addition to assessing compliance with the Privacy Act and APPs (discussed below), a PIA should also assess the broader privacy implications of a project. The OAIC recommends that APP entities consider the key questions set out below.

(a) Do individuals have to give up control of their personal information? s 42

(b) Will the project change the way individuals interact with the entity, such as through more frequent identity checks, costs, or impacts on individuals or groups who do not have identity documents? s 42

(c) Will decisions that have consequences for individuals be made as a result of the way personal information is handled in the project (such as decisions about services or benefits)? s 42

(d) How will the Department handle any privacy breaches or complaints?

s 42

(e) Are there audit and oversight mechanisms in place (including emergency procedures) in case the system fails?

s 42

(f) Does the project recognise the risk of function creep? (For example, is there an interest in using the personal information collected for the project for other purposes that might occur in the future?)

s 42

(g) How valuable would the information be to unauthorised users? (For example, is it information that others would pay money for or try to access via hacking?)

s 42

(h) Is any intrusion or surveillance fully justified and in proportion to the project's anticipated benefits? Is it the only way of achieving the aims of the project, and done in the least intrusive manner? Is it subject to legislative or judicial authority? What auditing and oversight measures are in place?

s 42

(i) How consistent is the project with community values about privacy?

s 42

s 42

s47E(d)

s47E(d)

s47E(d)

s 42

s 42

s 42

s 42

s 42

s 42

s 42

s 42

s 42

s 42

s 42

Glossary

Acronyms and Initialisms	
APP	Australian Privacy Principle
CRM	Customer Relationship Management
HBP	Health Business Partner
OAIC	Office of the Australian Information Commissioner
PIA	Privacy Impact Assessment

Definitions	
APP Guidelines or Guidelines	The APP Guidelines published by the OAIC at http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/ as revised on 2 March 2018. The APP Guidelines outline the mandatory requirements of the APPs, how the OAIC will interpret the APPs, and matters that may be taken into account when assessing an Agency's compliance with the Privacy Act and the APPs.
APP Entity	has the same meaning given under the *Privacy Act 1988* (Cth).
Approved Privacy Code	means an APP Code, as defined under section 26C of the Privacy Act.
Commonwealth entity	has the same meaning given under the *Public Governance, Performance and Accountability Act 2013* (Cth). This PIA also refers to Commonwealth entities as 'Agencies'.
Department	Department of Health
Enquiry Details	the following information which will be collected and stored by the Solution when an enquiry comes into the Contact Centre (regardless of the channel): (a) a Unique ID; (b) the incoming Line/Inbox; (c) Enquirer details (name, email, phone, address) or anonymous; and (d) Enquiry Sensitivity Rating
Issue Record	an Issue Record to be held in the Solution, containing the following details about the issue(s) raised by each enquiry: (a) Issue Type; (b) Issue Text; (c) Issue Outcome; and (d) Enquirer details (name, email, phone, address) or anonymous.
Organisation	has the same meaning given under section 6C of the Privacy Act.
Personal information	means information or an opinion 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, as defined in section 6 of the Privacy Act. Personal information may, in certain circumstances, include the following: (a) an email address (where that address contains a person's name);

	(b) an email address (in cases where that address does not contain a person's name, but the identity of the email account holder can be reasonably identified, including by reference to account-related information holdings); and (c) a telephone number (in cases where the person associated with the telephone number can be reasonably identified by reference to account-related information holdings).
Privacy Act	The *Privacy Act 1988* (Cth).
Project Description	The description of the Solution contained in section 5 of this PIA Report.
Sensitive information	means: (a) 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 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.

s 47E

Schedule 1

Information Flow Model

s47E(d)

Schedule 2

Australian Privacy Principles

Australian Privacy Principle 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;

(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.

Australian Privacy Principle 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.

Australian Privacy Principle 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 (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 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.

Australian Privacy Principle 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.

Australian Privacy Principle 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 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.

Australian Privacy Principle 6 — use or disclosure of Personal Information

Use or disclosure

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;

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.

Australian Privacy Principle 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.

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 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.

Australian Privacy Principle 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:

(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.

Australian Privacy Principle 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 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).

Australian Privacy Principle 10 — quality of Personal 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.

Australian Privacy Principle 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.

Australian Privacy Principle 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 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.

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.

Australian Privacy Principle 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 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 Information (as the case may be).