Chapter 6: Australian Privacy Principle 6 — Use or disclosure of personal information

Version 1.0, February 2014

Key points

- APP 6 outlines when an APP entity may use or disclose personal information.
- An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies.
- The exceptions include where:
    - the individual has consented to a secondary use or disclosure
    - the individual would reasonably expect the APP entity to use or disclose their personal information for the secondary purpose, and that purpose is related to the primary purpose of collection, or, in the case of sensitive information, directly related to the primary purpose
    - the secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order
    - a permitted general situation exists in relation to the secondary use or disclosure
    - the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure
    - the APP entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body, or
    - the APP entity is an agency (other than an enforcement body) and discloses biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3.

What does APP 6 say?

6.1 APP 6 outlines when an APP entity may use or disclose personal information. The intent is that an entity will generally use and disclose an individual's personal information only in ways the individual would expect or where one of the exceptions applies.

6.2 An APP entity that holds personal information about an individual can only use or disclose the information for a particular purpose for which it was collected (known as the 'primary purpose' of collection), unless an exception applies. Where an exception applies the entity may use or disclose personal information for another purpose (known as the 'secondary purpose'). Exceptions include:

- the individual consented to a secondary use or disclosure (APP 6.1(a))
- the individual would reasonably expect the secondary use or disclosure, and that is related to the primary purpose of collection or, in the case of sensitive information, directly related to the primary purpose (APP 6.2(a))

- the secondary use or disclosure of the personal information is required or authorised by or under an Australian law or a court/tribunal order (APP 6.2(b))
- a permitted general situation exists in relation to the secondary use or disclosure of the personal information by the APP entity (APP 6.2(c))
- the APP entity is an organisation and a permitted health situation exists in relation to the secondary use or disclosure of the personal information by the organisation (APP 6.2(d))
- the APP entity reasonably believes that the secondary use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body (APP 6.2(e))
- the APP entity is an agency (other than an enforcement body) and discloses personal information that is biometric information or biometric templates to an enforcement body, and the disclosure is conducted in accordance with guidelines made by the Information Commissioner for the purposes of APP 6.3 (APP 6.3).

6.3 An APP entity may disclose personal information, other than sensitive information, to a related body corporate (s 13B(1)(b)).

6.4 APP 6 does not apply to the use or disclosure by an organisation of:

- personal information for the purpose of direct marketing (this is covered by APP 7), or
- government related identifiers (this is covered by APP 9) (APP 6.7).

'Holds', 'use', 'disclose' and 'purpose'

6.5 Each of the terms 'holds', 'use', 'disclose' and 'purpose' which are used in APP 6 and other APPs, are discussed in more detail in Chapter B (Key concepts). The following is a brief analysis of the meaning of these terms in the context of APP 6.

'Holds'

6.6 APP 6 only applies to personal information that an APP entity 'holds'. An APP entity 'holds' personal information 'if the entity has possession or control of a record that contains the personal information' (s 6(1)).

6.7 The term 'holds' extends beyond physical possession of a record to include a record that an entity has the right or power to deal with. For example, an APP entity that outsources the storage of personal information to a third party, but retains the right to deal with that information, including to access and amend it, holds that personal information. The term 'holds' is discussed further in Chapter B (Key concepts).

'Use'

6.8 The term 'use' is not defined in the Privacy Act. An APP entity 'uses' information where it handles or undertakes an activity with the information, within the entity's effective control. For further discussion of use, see Chapter B (Key concepts). Examples include:

- the entity accessing and reading the personal information
- the entity searching records for the personal information
- the entity making a decision based on the personal information
- the entity passing the personal information from one part of the entity to another
- unauthorised access by an employee of the entity.[1]

'Disclose'

6.9 The term 'disclose' is not defined in the Privacy Act. An APP entity 'discloses' personal information where it makes it accessible to others outside the entity and releases the subsequent handling of the information from its effective control. This focuses on the act done by the disclosing party. The state of mind or intentions of the recipient does not affect the act of disclosure. Further, there will be a disclosure in these circumstances even where the information is already known to the recipient. For further discussion of disclosure, see Chapter B (Key concepts).

6.10 The release may be a proactive release or publication, a release in response to a specific request, an accidental release or an unauthorised release by an employee.[2] Examples include where an APP entity:

- shares the personal information with another entity or individual
- discloses personal information to themselves, but in their capacity as a different entity
- publishes the personal information on the internet, whether intentionally or not,[3] and it is accessible by another entity or individual
- accidentally provides personal information to an unintended recipient[4]
- reveals the personal information in the course of a conversation with a person outside the entity
- displays a computer screen so that the personal information can be read by another entity or individual, for example, at a reception counter or in an office.

6.11 'Disclosure' is a separate concept from:

- 'unauthorised access' which is addressed in APP 11. An APP entity is not taken to have disclosed personal information where a third party intentionally exploits the entity's security measures and gains unauthorised access to the information.[5]

[1] An APP entity is taken to have 'used' personal information where an employee gains unauthorised access 'in the performance of the duties of the person's employment' (see s 8(1)).

[2] An APP entity is taken to have 'disclosed' personal information where an employee carries out an unauthorised disclosure 'in the performance of the duties of the person's employment' (s 8(1)).

[3] See OAIC, *Own Motion Investigation Report — Medvet SciencePty Ltd*, July 2012, OAIC website <www.oaic.gov.au>; *Own Motion Investigation Report — Telstra Corporation Limited*, June 2012, OAIC website <www.oaic.gov.au>.

[4] The APP entity may also breach APP 11 if it did not take reasonable steps to protect the information from this unauthorised disclosure (see APP 11, Chapter 11).

[5] The actions of an employee will be attributed to the APP entity where it was carried out 'in the performance of the duties of the person's employment' (s 8(1)).

Examples include unauthorised access following a cyber-attack[6] or a theft, including where the third party then makes that personal information available to others outside the entity. However, where a third party gains unauthorised access, the APP entity may breach APP 11 if it did not take reasonable steps to protect the information from unauthorised access (see Chapter 11 (APP 11))

- 'use', which is discussed in paragraph 6.8 above. APP 6 generally imposes the same obligations on an APP entity for uses and disclosures of personal information. Therefore, this distinction is not relevant in interpreting this principle (except in relation to APP 6.3). However, the distinction is relevant to APP 8, which applies to the disclosure of personal information to an overseas recipient (see Chapter 8 (APP 8)).

'Purpose' of collection

6.12 The purpose for which an APP entity collects personal information is known as the 'primary purpose' of collection. This is the specific function or activity for which the entity collects the personal information. 'Purpose', including how to identify and describe the primary purpose, is discussed in more detail in Chapter B (Key concepts).

6.13 The notification requirements in APP 5 complement the limitations on use and disclosure under APP 6. APP 5 requires an APP entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. This includes the primary purpose of collection and could also include other purposes for which the entity collects the information (known as secondary purposes) (see APP 5.2(d)). The notification requirements are discussed in Chapter 5 (APP 5).

Using or disclosing personal information for a secondary purpose

6.14 A 'secondary purpose' is any purpose other than the primary purpose for which the APP entity collected the personal information.

6.15 The grounds on which an APP entity may use or disclose personal information for a secondary purpose are outlined below. It is nevertheless open to an entity not to rely on any such ground and to decide not to use or disclose personal information, unless the use or disclosure is required by law (see paragraphs 6.29–6.31 below).

Using or disclosing personal information with the individual's consent

6.16 APP 6.1(a) permits an APP entity to use or disclose personal information for a secondary purpose where the individual has consented to the use or disclosure.

6.17 Consent is defined in s 6(1) as 'express consent or implied consent' and is discussed in Chapter B (Key concepts). The four key elements of consent are:

[6] See OAIC, *Own Motion Investigation Report — Sony Playstation Network/ Qriocity*, September 2011, OAIC website <www.oaic.gov.au>.

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent.

Using or disclosing personal information where reasonably expected by the individual and related to the primary purpose of collection

6.18 APP 6.2(a) permits an APP entity to use or disclose personal information for a secondary purpose if the individual would reasonably expect the entity to use or disclose the information for that secondary purpose, and:

- if the information is sensitive information, the secondary purpose is directly related to the primary purpose of collection, or
- if the information is not sensitive information, the secondary purpose is related to the primary purpose of collection.

6.19 This exception creates a two-limb test which focuses both on the reasonable expectations of the individual, and the relationship between the primary and secondary purposes.

Reasonably expect

6.20 The 'reasonably expects' test is an objective one that has regard to what a reasonable person, who is properly informed, would expect in the circumstances. This is a question of fact in each individual case. It is the responsibility of the APP entity to be able to justify its conduct.

6.21 An APP entity should consider whether an individual would reasonably expect it to use or disclose for a secondary purpose only some of the personal information it holds about the individual, rather than all of the personal information it holds. The entity should only use or disclose the minimum amount of personal information sufficient for the secondary purpose. For example, an individual may not reasonably expect an entity that is investigating their complaint against a contractor to disclose the individual's residential address and home contact details to the contractor as part of its investigation. The individual would reasonably expect the entity to give the contractor only the minimum amount of personal information necessary to enable them to respond to the complaint.[7]

6.22 Examples of where an individual may reasonably expect their personal information to be used or disclosed for a secondary purpose include where:

- the individual makes adverse comments in the media about the way an APP entity has treated them. In these circumstances, it may be reasonable to expect that the

[7] For another example of where an individual would not reasonably expect disclosure, see *W v Telecommunications Company* [2007] PrivCmrA 25, Australasian Legal Information Institute website <www.austlii.edu.au>.

entity may respond publicly to these comments in a way that reveals personal information specifically relevant to the issues that the individual has raised[8]

- an agency discloses to another agency a query, view or representation that an individual has made to the first-mentioned agency[9]
- the entity has notified the individual of the particular secondary purpose under APP 5.1 (see Chapter 5 (APP 5))
- the secondary purpose is a normal internal business practice, such as as auditing, business planning, billing or de-identifying the personal information.

Relationship between the primary and secondary purpose

6.23 This exception is limited to using or disclosing personal information for a secondary purpose that is 'related', or for sensitive information 'directly related', to the primary purpose of collection.

Related secondary purpose

6.24 A related secondary purpose is one which is connected to or associated with the primary purpose. There must be more than a tenuous link.[10]

6.25 Examples of where a secondary purpose is related to the primary purpose of collection include:

- an organisation collects personal information about an individual for the primary purpose of collecting a debt. A law firm, acting on behalf of that organisation in relation to the debt collection, contacts the individual's neighbour and seeks information from the neighbour about the individual's whereabouts (but does not disclose any specific information about the debt). This disclosure to the neighbour, for the secondary purpose of locating the individual, is related to the primary purpose of debt collection and would be within the individual's reasonable expectations[11]
- an agency collects personal information to include in an employee's personnel file for the primary purpose of administering that individual's employment.[12] It then uses this personal information as part of an investigation into complaints by the individual about working conditions. In these circumstances, the use for the secondary purpose of investigating a complaint in the workplace is related to the

[8] See *L v Commonwealth Agency* [2010] PrivCmrA 14 (24 December 2010), Australasian Legal Information Institute website <www.austlii.edu.au>.
[9] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 78.
[10] For examples of where disclosure of personal information for a secondary purpose is not related to the primary purpose of collection, see *B v Hotel* [2008] PrivCmrA 2, Australasian Legal Information Institute website <www.austlii.edu.au>; *E v Insurance Company* [2011] PrivCmrA 5, Australasian Legal Information Institute website <www.austlii.edu.au>.
[11] This example is adapted from *M and Law Firm* [2011] AICmrCN 7 (available at Australasian Legal Information Institute website <www.austlii.edu.au>), where the Commissioner also referred the complaint to the Australian Competition and Consumer Commission to consider whether the debt collection practices were consistent with its debt collection guidelines.
[12] The exemption relating to employee records in s 7B(3) only applies to organisations.

primary purpose of collection, and would be within the individual's reasonable expectations[13]

- an APP entity uses personal information for the purpose of de-identifying the information.

Directly related secondary purpose

6.26 For the use or disclosure of sensitive information, the secondary purpose must be 'directly related' to the primary purpose of collection. A directly related secondary purpose is one which is closely associated with the primary purpose, even if it is not strictly necessary to achieve that primary purpose. This requirement for a direct relationship recognises that the use and disclosure of sensitive information can have serious ramifications for the individual or their associates, including humiliation, embarrassment or loss of dignity.

6.27 An example of where a secondary purpose is directly related to the primary purpose of collection is:

- a health service provider collects health information about an individual for the purpose of providing treatment, and then decides, for ethical and therapeutic reasons, that they cannot treat the individual. The health service provider then advises another provider at the medical clinic of the individual's need for treatment and of the provider's inability to provide that treatment. This disclosure to the other provider is directly related to the purpose for which the information was collected, and would be within the individual's reasonable expectations.[14]

6.28 The use of sensitive information for the purpose of de-identifying the information will also be directly related to the primary purpose of collection.

Using or disclosing personal information as required or authorised by law

6.29 An APP entity may use or disclose personal information for a secondary purpose if the use or disclosure is required or authorised by or under an Australian law or a court/tribunal order (APP 6.2(b)).

6.30 The meaning of 'required or authorised by or under an Australian law or a court/tribunal order' is discussed in Chapter B (Key concepts).

6.31 Examples of where an APP entity may be required or authorised by law to use or disclose personal information include where:

- a warrant, order or notice issued by a court requires the entity to provide information, or produce records or documents that are held by the entity
- the entity is subject to a statutory requirement to report certain matters to an agency or enforcement body, for example, specific financial transactions, notifiable diseases and suspected cases of child abuse

[13] *N v Commonwealth Agency* [2009] PrivCmrA 17, Australasian Legal Information Institute website <www.austlii.edu.au>.
[14] *F v Medical Specialist* [2009] PrivCmrA 8, Australasian Legal Information Institute website <www.austlii.edu.au>.

- a law applying to the entity clearly and specifically authorises it to use or disclose the personal information, for example:
    - to give a record to the Private Health Insurance Ombudsman,[15] or to disclose matters to a trustee conducting a bankruptcy investigation[16]
    - a specified use or disclosure of personal information by an Agency Head, the Merit Protection Commissioner or the Australian Public Service Commissioner[17]
    - a specified use or disclosure of personal information under the Privacy Act, for example, to de-identify personal information as required by APP 11.

Using or disclosing personal information where a permitted general situation exists

6.32 An APP entity may use or disclose personal information for a secondary purpose if a 'permitted general situation' exists in relation to the use or disclosure of the information by the entity (APP 6.2(c)).

6.33 Section 16A lists seven permitted general situations (two of which only apply to agencies). The seven situations are set out below, and are discussed in Chapter C (Permitted general situations), including the meaning of relevant terms.

Lessening or preventing a serious threat to life, health or safety

6.34 An APP entity may use or disclose personal information for a secondary purpose where:

- it is unreasonable or impracticable to obtain the individual's consent to the use or disclosure, and
- the entity reasonably believes the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety (s 16A(1), Item 1).

6.35 Examples of where this permitted general situation might apply include:

- where an individual is seriously injured while interstate and, due to their injuries, cannot give informed consent, the individual's usual health service provider may be able to disclose personal information about the individual to another health service provider who is treating the individual's serious injuries on the basis that it is impracticable to obtain the individual's consent
- where an APP entity that provides child protection services has evidence that a child is at risk of physical or sexual abuse by their parent, the entity may be able to disclose the personal information of the parent to another child protection service on the basis that it would be unreasonable to obtain the parent's consent.

[15] *Private Health Insurance Act 2007*, s 250.10.
[16] *Bankruptcy Act 1966*, s 77A.
[17] *Public Service Act 1999*, s 72E and Public Service Regulations 1999, regulation 9.2.

Taking appropriate action in relation to suspected unlawful activity or serious misconduct

6.36 An APP entity may use or disclose personal information for a secondary purpose where the entity:

- has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in, and
- reasonably believes that the collection use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter (s 16A(1), Item 2).

6.37 Examples of where this permitted general situation might apply are the use of personal information by:

- an APP entity that is investigating fraudulent conduct by a professional adviser or a client in relation to the entity's functions or activities
- an agency that is investigating a suspected serious breach by a staff member of the Australian Public Service Code of Conduct.

Locating a person reported as missing

6.38 An APP entity may use or disclose personal information for a secondary purpose where the entity:

- reasonably believes that the use or disclosure is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing, and
- the use or disclosure complies with rules made by the Commissioner under s 16A(2) (s 16A(1), Item 3).

Reasonably necessary for establishing, exercising or defending a legal or equitable claim

6.39 An APP entity may use or disclose personal information for a secondary purpose where the use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim (s 16A(1) Item 4).

6.40 An example of where this permitted general situation might apply is where an individual has made a claim under their life insurance policy and the insurer is preparing to dispute the claim. The insurer may use or disclose personal information about the individual to establish its defence of the claim.

Reasonably necessary for a confidential alternative dispute resolution processes

6.41 An APP entity may use or disclose personal information for a secondary purpose where the use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution (ADR) process (s 16A(1), Item 5).

6.42 An example of where this permitted general situation might apply is where an APP entity discloses their version of events during a confidential ADR process, where that account includes the disclosure of personal information about an individual who is

directly or indirectly involved in the dispute. This permitted general situation will only apply where the parties to the dispute and the ADR provider are bound by confidentiality obligations.

Necessary for a diplomatic or consular function or activity

6.43 An agency may use or disclose personal information for a secondary purpose where the agency reasonably believes that the use or disclosure is necessary for the agency's diplomatic or consular functions or activities (s 16A(1), Item 6). This permitted general situation applies only to agencies, and not to organisations.

6.44 An example of where this permitted general situation might apply is where an agency with diplomatic or consular functions uses or discloses personal information to grant a diplomatic visa to a foreign national accredited as a member of the diplomatic staff of a mission to Australia.

Necessary for certain Defence Force activities outside Australia

6.45 The Defence Force (as defined in s 6(1)) may use or disclose personal information for a secondary purpose where it reasonably believes that the use or disclosure is necessary for a warlike operation, peacekeeping, civil aid, humanitarian assistance, a medical emergency, a civil emergency or disaster relief occurring outside Australia and the external Territories (s 16A(1), Item 7).

6.46 An example of where this permitted general situation might apply is where the Defence Force uses and discloses personal information about an enemy or other hostile adversary in order to support military operations.

Using or disclosing personal information where a permitted health situation exists

6.47 An organisation may use or disclose personal information if a 'permitted health situation' exists in relation to the use or disclosure (APP 6.2(d)). This exception applies only to organisations, and not to agencies.

6.48 Section 16B lists three permitted health situations that relate to the use or disclosure of health information or genetic information by an organisation. The three situations are set out below, and are discussed in Chapter D (Permitted health situations), including the meaning of relevant terms.

Conducting research; compiling or analysing statistics; management, funding or monitoring of a health service

6.49 An organisation may use or disclose health information about an individual for a secondary purpose if the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety, and:

- it is impracticable to obtain the individual's consent to the use or disclosure

- the use or disclosure is conducted in accordance with guidelines approved under s 95A,[18] and
- in the case of disclosure, the organisation reasonably believes that the recipient of the information will not disclose the information, or personal information derived from that information (s 16B(3)).

6.50 An example of where this permitted health situation might apply is where an organisation discloses health information to a researcher who is conducting public health research in circumstances where the age of the information makes it impracticable to obtain consent. The disclosing organisation should have a written agreement with the researcher which requires the researcher not to disclose the health information, or any personal information that is derived from that health information. The disclosure must be carried out in accordance with guidelines approved under s 95A.

Necessary to prevent a serious threat to the life, health or safety of a genetic relative

6.51 An organisation may use or disclose genetic information about an individual for a secondary purpose if:

- the organisation has obtained the information in the course of providing a health service to the individual
- the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the individual
- the use or disclosure is conducted in accordance with guidelines approved under s 95AA,[19] and
- in the case of disclosure, the recipient of the information is a genetic relative of the individual (s 16B(4)).

6.52 An example of where this permitted health situation might apply is:

- in the course of providing a health service, an organisation obtains information that a patient has a pathogenic mutation in the Huntington disease gene, and
- the individual refuses to consent to the organisation disclosing any information to their genetic relatives, even after the individual has participated in discussions and counselling, and received information about the implications of the diagnosis for the individual's genetic relatives
- despite this refusal, the organisation may disclose the genetic information to genetic relatives under this exception, providing any disclosure is in accordance with the guidelines approved under s95AA.

[18] See National Health and Medical Research Council (NHMRC), *Guidelines approved under Section 95A of the Privacy Act 1988,* NHMRC website <www.nhmrc.gov.au>.

[19] See National Health and Medical Research Council (NHMRC), *Use and disclosure of genetic information to a patient's genetic relatives under Section 95AA of the Privacy Act 1988: Guidelines for health practitioners in the private sector,* NHMRC website <www.nhmrc.gov.au>.

Disclosure to a responsible person for the individual

6.53 An organisation may disclose health information about an individual for a secondary purpose if:

- the organisation provides a health service to the individual
- the recipient of the information is a 'responsible person' for the individual
- the individual is either physically or legally incapable of giving consent to the disclosure, or physically cannot communicate consent to the disclosure
- the individual providing the health service (the 'carer') is satisfied that either the disclosure is necessary to provide appropriate care or treatment of the individual, or the disclosure is made for compassionate reasons
- the disclosure is not contrary to any wish expressed by the individual before the individual became unable to give or communicate consent of which the carer is aware or of which the carer could reasonably be expected to be aware
- the disclosure is limited to the extent reasonable and necessary for providing appropriate care or fulfilling compassionate reasons (s 16B(5)).

6.54 An example of where this permitted health situation might apply is where an individual who cannot give consent is released from hospital into the care of family members. The health service provider (referred to in this exception as the 'carer') discloses health information to the family members to enable them to monitor the individual's progress and administer medication. In these circumstances, the exception would apply where the carer is satisfied that the disclosure is necessary to provide appropriate care for the individual. The disclosure must be limited to the extent reasonable and necessary to provide appropriate care.

6.55 Another example is where a carer discloses health information to an unconscious patient's family members about the patient's condition. In these circumstances, the exception would apply where the carer is satisfied that the disclosure is necessary for compassionate reasons. The disclosure must be limited to the extent reasonable and necessary for the compassionate reasons.

Using or disclosing personal information for an enforcement related activity

6.56 An APP entity may use or disclose personal information for a secondary purpose where the entity reasonably believes that the use or disclosure of the personal information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body (APP 6.2(e)).

6.57 'Enforcement body' is defined in s 6(1) as a list of specific bodies and is discussed in Chapter B (Key concepts). The list includes Commonwealth, State and Territory bodies that are responsible for policing, criminal investigations, and administering laws to protect the public revenue or to impose penalties or sanctions. Examples of Commonwealth enforcement bodies are the Australian Federal Police, Australian Crime

Commission, Customs, the Integrity Commissioner,[20] the Immigration Department,[21] Australian Prudential Regulation Authority, the Australian Securities and Investments Commission and AUSTRAC.

6.58 'Enforcement related activities' is defined in s 6(1) and is discussed in Chapter B (Key concepts). Enforcement related activities include the prevention, detection, investigation and prosecution or punishment of criminal offences and intelligence gathering activities.

Reasonable belief

6.59 The phrase 'reasonable belief' is discussed in Chapter B (Key concepts). In summary, the APP entity must have a reasonable basis for the belief, and not merely a genuine or subjective belief. It is the responsibility of the entity to be able to justify its reasonable belief.

6.60 In some circumstances, the basis for an APP entity's 'reasonable belief' will be clear, for example, if the entity discloses personal information in response to a written request by an enforcement body and the request is dated and signed by an authorised person. In other circumstances, the basis for this belief may be less clear, and the entity will need to reflect more carefully about whether its judgment is reasonable.

Reasonably necessary

6.61 The 'reasonably necessary' test is an objective test: whether a reasonable person who is properly informed would agree that the use or disclosure is reasonable in the circumstances. Again, it is the responsibility of an APP entity to be able to justify that the particular use or disclosure is reasonably necessary.

6.62 For example, investigators from an enforcement body suspect that a particular building is being used for drug trafficking activities. As part of the enforcement body's intelligence gathering, the investigators request an APP entity to disclose the personal information of individuals associated with the building (although the investigators do not know the extent, if any, of the involvement of the individuals). This disclosure would be 'reasonably necessary' as it forms an important part of the enforcement body's intelligence gathering about the suspected drug trafficking.

6.63 The use or disclosure does not need to relate to an existing enforcement related activity. The use or disclosure may be reasonably necessary for the initiation of an enforcement related activity. This recognises that a law enforcement body may not be in a position to prevent, detect or investigate offences or breaches of the law, unless and until certain information, including personal information, is brought to its attention.

6.64 An APP entity should ensure that it only uses or discloses the minimum amount of personal information reasonably necessary for a particular enforcement related activity. For example, an entity may hold a range of personal information about an individual, such as the person's contact details, their photograph and information about their

[20] 'Integrity Commissioner is defined in s 6(1) as having the same meaning as in the *Law Enforcement Integrity Commissioner Act 2006.*

[21] 'Immigration Department' is defined in s 6(1) as the Department administered by the Minister administering the *Migration Act 1958*.

political views and religious views. Before disclosing all of this personal information to the enforcement body, the entity should consider whether only some of it is reasonably necessary for the enforcement related activity. If so, it should disclose only that information.

Making a written note of use or disclosure for this secondary purpose

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

6.66 The APP entity could include the following details in that note:

- the date of the use or disclosure
- details of the personal information that was used or disclosed
- the enforcement body conducting the enforcement related activity
- if the entity used the personal information, how the personal information was used by the entity
- if the entity disclosed the personal information, who it disclosed the personal information to (this may be the enforcement body or another entity)
- the basis for the entity's 'reasonable belief'. This will help the entity assure itself that this exception applies, and it may be a useful reference if the entity later needs to justify its reasonable belief.

6.67 This requirement does not apply where a law prohibits the APP entity from making such a record.

Disclosing biometric information to an enforcement body

6.68 An agency may disclose biometric information or biometric templates for a secondary purpose if:

- the agency is not an enforcement body, and
- the recipient of the information is an enforcement body, and
- the disclosure is conducted in accordance with guidelines made by the Commissioner for the purposes of APP 6.3 (see APP 6.3, Chapter 6).

6.69 This exception does not apply to organisations.

6.70 'Biometric information' and 'biometric templates' are types of 'sensitive information' (defined in s 6(1)). 'Enforcement body' is defined in s 6(1) and is discussed in more detail in Chapter B (Key concepts).

De-identifying certain health information before disclosure

6.71 APP 6.4 applies where an organisation collects health information under an exception to APP 3 in s 16B(2). Section 16B(2) outlines the permitted health situation that

allows an organisation to collect health information about an individual if the collection is necessary for research relevant to public health or safety, the compilation or analysis of statistics relevant to public health or public safety, or the management, funding or monitoring of a health service and certain other criteria are satisfied (see Chapter D (Permitted health situations)).

6.72 In these circumstances, APP 6.4 requires the organisation to take reasonable steps to ensure that the information is de-identified, before it discloses the information in accordance with APPs 6.1 or 6.2.

6.73 Personal information is de-identified 'if the information is no longer about an identifiable individual or an individual who is reasonably identifiable' (s 6(1)). De-identification is discussed in more detail in Chapter B (Key concepts).[22]

6.74 The reasonable steps that an organisation should take will depend upon circumstances that include:

- the possible adverse consequences for an individual if their health information is not de-identified before it is disclosed. More rigorous steps may be required as the risk of adversity increases
- the practicability, including time and cost involved. However, an organisation is not excused from taking particular steps to de-identify health information by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.

Related bodies corporate

Disclosing personal information to a related body corporate

6.75 Section 13B(1)(b) provides that where a body corporate discloses personal information (other than sensitive information) to a related body corporate, this is generally not considered 'an interference with the privacy of an individual' under the Privacy Act (interferences with privacy are discussed in Chapter A (Introductory matters)). This provision applies to related bodies corporate and not to other corporate relationships, such as a franchise or joint-venture relationship.[23]

6.76 The effect of this provision is that an APP entity may disclose personal information (other than sensitive information) to a related body corporate without relying on an exception in APP 6.2.

[22] See also, OAIC *Privacy Business Resource — De-identification of Data and Information* and *Information Policy Agency Resource — De-identification of Data and Information*, OAIC website <www.oaic.gov.au>.

[23] Section 6(8) states 'for the purposes of this Act, the question of whether bodies corporate are related to each other is determined in the manner in which that question is determined under the *Corporations Act 2001*'.

Using or disclosing personal information collected from a related body corporate

6.77 An APP entity that collects personal information from a related body corporate is taken to have the same primary purpose of collection as its related body corporate (APP 6.6). Under APP 6, the entity may only use or disclose the personal information for that primary purpose, unless an exception to that principle applies (see paragraph 6.2 above).

For example, an APP entity collects personal information about an applicant contractor for the purpose of assessing their suitability to perform work on its behalf. The parent company then collects that personal information from the entity. The primary purpose of this collection is taken to be the same as the original purpose of collection. The parent company may only disclose the personal information to a third party for another purpose, where an exception to APP 6 applies.