AUSTRALIAN COMMISSION ON SAFETY AND QUALITY IN HEALTH CARE

# Privacy Policy

July 2022

**Version 1.8**

# Document Information

## Version History

| Version | Issue Date | Author | Reviewers | Outcome of Review |
|---|---|---|---|---|
| v0.1 | May 2014 | Jason Whatley | Mike Wallace, Chief Operating Officer | Drafted |
| v0.2 | May 2014 | Jason Whatley | Neville Board, Director, Information Strategy | Alignment with national health data policies and arrangements |
| v1.0 | June 2014 | Jason Whatley | Audit And Risk Committee<br>Board | Endorsed<br>Approved on 7 August 2014 |
| v1.1 | May 2017 | Stan Ahn | Mike Wallace, Chief Operating Officer | Annual review |
| v1.2 | Feb 2018 | Stan Ahn<br>Lisa Murphy<br>Damen Pearce | Catherine Katz, Chief Privacy Officer<br>Mike Wallace, Chief Operating Officer | Included the Commission's privacy framework and added the Commission's management of the Notifiable Data Breaches Scheme.<br>Approved at the 21 February2018 meeting. |
| v1.3 | Dec 2018 | Stan Ahn | | Included D Pearce as one of the privacy officers. |
| v1.4 | Mar 2019 | Stan Ahn | Catherine Katz, Chief Privacy Officer<br>Mike Wallace, Chief Operating Officer | Included a new paragraph on joint notifiable data breaches.<br>Included a new section on the Commission's Privacy Management Plan.<br>Approved<br>Approved |
| v1.5 | Feb 2021 | Stan Ahn | | Periodic review. Minor typographical corrections and updates to hyperlinks. |
| v1.6 | Oct 2021 | Stan Ahn | | Updated Document Ownership Details with Chris Leahy as the COO. |
| v1.7 | Mar 2022 | Stan Ahn | Catherine Katz, Chief Privacy Officer<br>Chris Leahy, Chief Operating Officer | Included process for conducting Privacy Impact Assessments.<br>Approved<br>Approved |
| v1.8 | Jul 2022 | Stan Ahn | Catherine Katz, Chief Privacy Officer<br>Mike Wallace, acting Chief Operating Officer | Updated the Commission's Privacy Officers<br>Approved, 6 July 2022<br>Approved, 6 July 2022 |

## Ownership

Enquiries regarding this document can be made to:

| | |
|---|---|
| **Name:** | Chris Leahy |
| **Position:** | Chief Operating Officer |
| **Email:** | christopher.leahy@safetyandquality.gov.au |
| **Phone:** | 02 9126 3600 |

## Document Location

An electronic copy of this document is stored in the Commission's electronic document management system at TRIM D14-15168.

## Date for Next Review

This policy will be reviewed annually or as required.

# Glossary

| | |
|---|---|
| APPs | means the 13 Australian Privacy Principles under the Privacy Act |
| APS Privacy Governance Code | means the Privacy (Australian Public Service – Governance) APP code 2018 to be implemented by the OAIC |
| Commission | means the Australian Commission on Safety and Quality in Health Care |
| Healthcare information | means:<br>• information collected in connection with the provision of a health service<br>• information or opinion about the health or disability of an individual<br>• an individual's expressed wishes about the provision of health services<br>• any information about health services provided to an individual |
| NDB | means Notifiable Data Breaches |
| NDB scheme | means the *Privacy Amendment (Notifiable Data Breaches) Act 2017* which will come into effect from 22 February 2018 and will introduce an obligation for agencies to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm |
| NHR Act | means the *National Health Reform Act 2011* |
| OAIC | means the Office of the Australian Information Commissioner |
| Personal information | is defined by the Privacy Act and means information or an opinion about an identified individual, or an individual who is reasonably identifiable |
| PIA | means Privacy Impact Assessment |
| Privacy Act | means the *Privacy Act 1988* |
| Sensitive information | is defined by the Privacy Act and means information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record that is also personal information, or health information or, genetic information about an individual, or certain biometric information. |
| The Policy | means this Privacy Policy. |

# Introduction

The Australian Commission on Safety and Quality in Health Care (the Commission) is committed to the protection of personal information in a manner consistent with the *Privacy Act 1988 (*Privacy Act*)* and the Australian Privacy Principles (APPs).

The Commission is also committed to ensuring that healthcare information accessed for the purpose of fulfilling the Commission's functions under the National Health Reform Act 2011 (NHR Act) and the National Health Reform Agreement (NHRA) are managed in a manner that is consistent with the APPs and the state and territory privacy laws and healthcare regulation.

The Commission's privacy arrangements including this Policy and its internal procedures are periodically audited by the Commission's internal auditors.

When necessary, the Commission will review and revise this Policy. Up to date version of the Policy will be available from the Commission's website (http://www.safetyandquality.gov.au).

# Privacy Framework

The Commission is committed to protecting personal information, consultation feedback and healthcare information, ensuring appropriate use, management, access and storage. The Policy provides the structure in which information is collected and considered under the requirements of the Privacy Act. A number of other supporting policies and frameworks have been developed to supplement the principles outlined in the Policy. These include:

- Data Governance Framework and the Data Plan
- Privacy Policy
- Agency Security Plan

Together, these form the Commission's privacy framework that governs the Commission's treatment of information and their privacy.

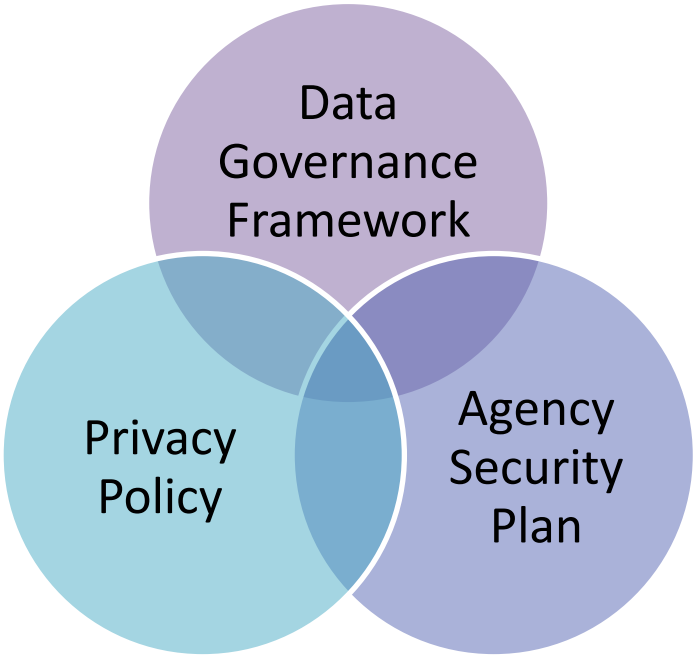


**Figure 1 - Commission's privacy framework**

The Commission has developed and maintains supplementary policies and frameworks to manage and administer different types of information.

## Resources

Other resources relevant to this Policy include the following:

- Privacy Act (www.comlaw.gov.au)
- NHR Act (www.comlaw.gov.au)
- NHRA (https://www.federalfinancialrelations.gov.au/)
- Notifiable Data Breaches scheme (www.oaic.gov.au)
- Australian Government Agencies Privacy Code (www.oaic.gov.au)
- Privacy Impact Assessments (www.oaic.gov.au)

## Scope

This Policy applies to personal information collected by the Commission. The requirements under this Policy applies to all employees and contractors employed or engaged by the Commission.

## Purpose

The Policy is intended to provide information on the following:

- What information is collected by the Commission.
- How the Commission collects and holds personal information.
- How the Commission use personal information.
- How the Commission handles data breaches that include personal information.
- The Commission's treatment of the APPs' requirements.

The Policy also informs individuals how they may access their personal information collected by the Commission and request corrections if necessary. The Policy also advises how individuals may lodge complaints regarding the Commission's conduct with personal information.

## Definition of 'personal information'

Personal information is defined in the Privacy Act as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable'.[1]

What constitutes personal information will vary depending on whether an individual can be identified or is reasonably identifiable in the particular circumstance. Whether an individual is 'reasonably identifiable' from particular information about that individual will depend on factors such as the nature and the extent of the information and whether it is possible for the recipient of the information to identify the individual using available resources (including other information available to that recipient). The cost, difficulty, practicality and likelihood of a person or an entity identifying an individual are also relevant to deciding whether they are 'reasonably identifiable'.

Where it is technically possible to identify an individual based on the information, but doing so is not practicable, that individual will generally be regarded as not 'reasonably identifiable'. For example, if the cost of reasonably identifying an individual is overly

[1] https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/

expensive or resource intensive, that individual would be regarded as not reasonable identifiable.

The definition of personal information only relates to natural persons. In most circumstances it will not apply to deceased persons and it does not extend to other legal persons such as companies.

## Type of information collected by the Commission

**Personal information**

The Commission only collects personal information where the information is reasonably necessary for, or directly related to, one or more of the Commission's functions or activities. Examples include names, addresses, phone numbers, email addresses, other contact details, employment history, educational qualifications, procurement records, consultancy records, committee membership details, bank account details, superannuation details, creditor and debtor information, recruitment records and personnel records. This information is subject to the Privacy Act and the Commission treats such information in a manner consistent with that Act.

At times the Commission may also collect personal information from third parties or publicly available records. However, the Commission will only do so if after obtaining expressly or impliedly consent, unless it is unreasonable or impracticable to collect that information from the person or where the Commission is required or authorised to do so under Australian law or court or tribunal order.

**Healthcare information**

Under the National Health Information Agreement, the Commission is responsible for collecting, analysing, interpreting and disseminating information related to health care safety and quality, as well as for identifying indicators related to safety and quality. To achieve this function, the Commission requires timely access to healthcare information. The Commission's healthcare data requirements are outlined in the Commission's Data Plan, which has been prepared in accordance with section B85 of the NHRA.

The Commission's arrangements relating to the use of healthcare information is not covered by this Privacy Policy. Healthcare information is considered a subset of personal information and is treated as 'protected Commission information' under the NHRA.

The use of healthcare data is outlined in the Commission's Data Governance Framework. This framework is supported by a number of policies and procedures to support the effective and appropriate use of healthcare information. These are made available on request.

## Collecting and holding personal information

When seeking personal information, the Commission informs the individual the purpose for collecting the information, the Commission's requirements to access the information, how the information will be stored, the ramifications if the Commission fails to collect the information and whether the information is required under Australian law.

If the Commission receives unsolicited personal information, the Commission will determine whether that information could have been collected in accordance with the APPs. If the Commission determines that the information could not have been obtained in accordance with the APPs, the Commission will consider whether it is obliged to retain that information. If not, the Commission will destroy the information or ensure that the information is de-identified if it is lawful and reasonable to do so.

The Commission uses TRIM as its official electronic records management system for storing of its information, including personal information. TRIM is a secure environment vetted and managed by the Australian Government Department of Health and meets the security requirements of the Australian Government.

## Using personal information

The Commission uses personal information to enable it to undertake a range of business-related activities. These activities are administrative in nature and can be grouped into three categories:

### Committee files

The NHR Act authorises the Commission to establish committees to provide advice or assist in performing its functions.

The Commission collects and uses personal information relating to such committee members in order to establish and maintain these committees. Personal information contained in committee files may include contact details and terms of engagement.

If the Commission is required to pay sitting fees to eligible committee members, the Commission also collects and uses their bank accounts, taxation details and superannuation details in order to act as their employer and pay their sitting fees.

### Personnel files

The Commission collects and uses personnel files in order to carry out the functions necessary as an employer. Personal information in these files may include applications for employment; terms of employment; records relating to employee's salary, benefits and leave; medical certificates or health related information; any criminal records; contact details; taxation details and superannuation contributions.

### Personal information in relation to consultation

The Commission routinely collects consultation feedback on a variety of program areas. This can be in the form of written submissions via an online survey platform or through a focus group environment. Names, email address, phone numbers, details of workplaces and opinions are collated and analysed to inform safety and quality initiatives. All personal information is de-identified for external use and is treated in line with this Policy.

### Corporate information

In addition to the above categories, the Commission collects and uses corporate information that may contain information relating to a person in their corporate capacity. Examples of such information include contact details and job titles.

Corporate information does not meet the definition of personal information under the Privacy Act. The Commission treats such information as commercial-in-confidence if it is appropriate to do so.

## Disclosure of personal information

The Commission discloses personal information to other organisations or government agencies after the individual has been advised, or would reasonably expect, that their information will be disclosed to the receiving entity for the purpose of the Commission undertaking its activities as an employer. An example of such scenario includes disclosure of a staff member's personal information to the Australian Government Department of Health for payroll purposes.

If a disclosure of personal information is required that an individual would not reasonably expect to be required, the Commission will seek the individual's consent prior to the disclosure.

The Commission will only disclose personal information if permitted under APP 6 – Use and disclosure of personal information.

## Quality and security of personal information

The Commission will take reasonable steps to ensure that personal information held by the Commission is accurate, current, complete and relevant. The Commission will destroy or de-identify personal information if it is no longer necessary and its retention is not required under Australian law. The Commission will also ensure that personal information is reasonably protected from misuse, interference, loss and from unauthorised access, modification or disclosure through a range of physical and electronic security measures including restricted physical access to the Commission's premises, security firewalls and computer user identifiers and passwords.

The Commission applies the principles set out in the Australian Government Protective Security Policy Framework (PSPF) and Australian Government Information Security Manual (ISM) with reference to the Commission's individual security requirements.

The Commission's Agency Security Plan is consistent with the PSPF and ISM and takes other guidance into consideration including the management of emerging threats, new direction(s) from the Attorney-General's Policy forum, the Privacy Act, APS Code of Conduct, Workplace Health and Safety Act and the Commission's Risk Management Framework.

## Privacy or data breach

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* established the Notifiable Data Breaches (NDB) scheme in Australia. The NDB scheme applies to all agencies including the Commission from 22 February 2018.

The NDB scheme will introduce an obligation for agencies to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm. In this context, serious harm refers to serious physical, psychological, emotional, financial or reputational harm to an individual or individuals.

The Commission will manage all data breaches in accordance with the NDB. Figure 1 illustrates the Commission's process for managing NDB.

If a suspected or known data breach occurs, the Commission's Privacy Officers will initially respond and work with the affected area to contain further access or disclosure of the data. The Privacy Officers will then work with the Chief Privacy Officer and the Chief Operating Officer to determine whether serious harm is likely from the suspected or known breach.

If serious harm is likely from the data breach, the Commission will immediately notify the affected individuals to advise that a suspected or known data breach has occurred which includes their personal information, and actions are being undertaken to limit or mitigate the harm as much as possible.

The Commission will also prepare a statement to the OAIC via the NDB Statement – Form (available from www.oaic.gov.au) notifying the following to the OAIC:

- The Commission's identity and its contact details.
- A description of the breach and actions being undertaken to limit the breach.

- The type of information concerned.
- Recommended steps for the affected individuals.

The Commission will then work with OAIC on any recommendations or directions from the Information Commissioner relating to the breach.

The Commission will review the incident to determine possible causes of the breach and revise its internal policies and/or procedures to prevent reoccurrence. Possible actions will include updating policies and procedures relating to records management, updating the Commission's Agency Security Plan and additional staff training on privacy.

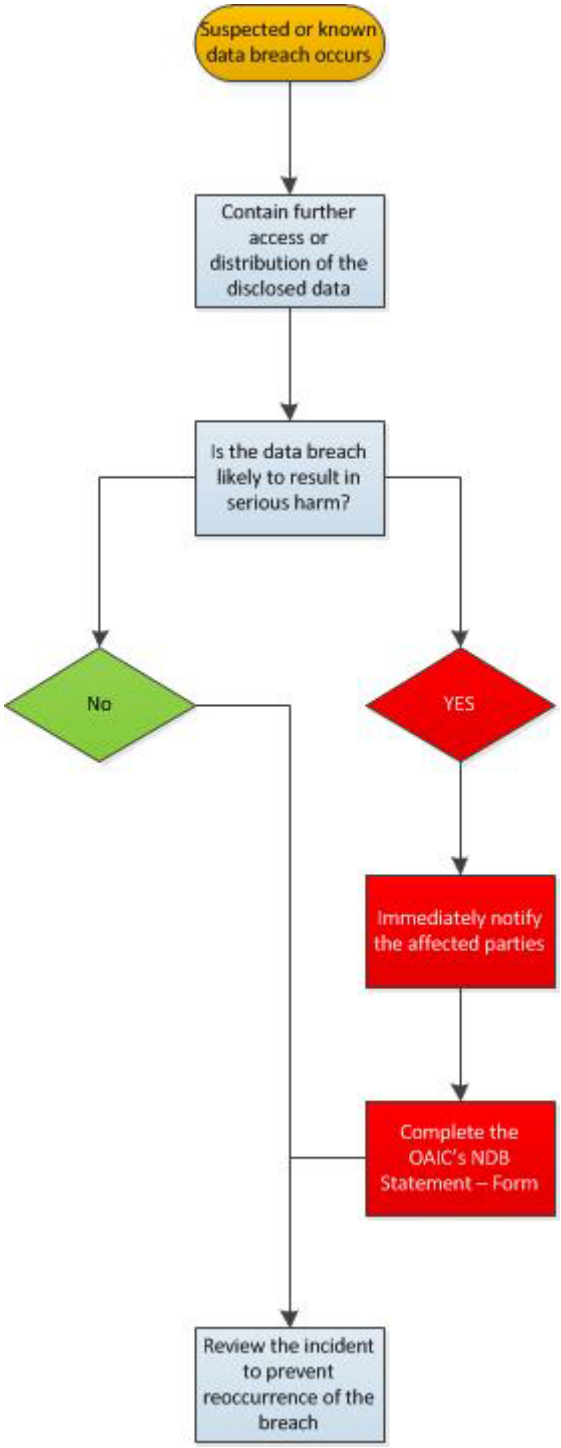


**Figure 2 - Commission's process for the NDB scheme**

If the breach relates to data held jointly by the Commission and organisations, the Commission will work with the relevant organisations to jointly review the breach and develop an appropriate joint strategy as per the OAIC's advice on joint NDBs.[2]

## Privacy Management Plan

Under section 9 of the *Privacy (Australian Government Agencies – Governance) APP Code 2017*, the Commission is required to develop and maintain a Privacy Management Plan that identifies specific, measurable privacy goals and targets. The plan must also set out how the Commission will meet its privacy obligations under the Australian Privacy Principles (APPs).

The Commission's Privacy Management Plan is at D18-33607. The Commission's Chief Privacy Officer is responsible for maintaining this plan with assistance from the Privacy Officers.

## Privacy Impact Assessments

The *Privacy (Australian Government Agencies – Governance) APP Code 2017* requires agencies subject to the Privacy Act to conduct a Privacy Impact Assessment (PIA) for all 'high privacy risk projects' or when instructed to do so by the OAIC.

The Commission determines which of its projects are considered 'high privacy risk' by completing the ACSQHC Privacy Impact Assessment Threshold (D22-7266) for a project that has, or is anticipated to have, a privacy risk element. A project that is determined by the assessment as a high privacy risk must complete the ACSQHC Privacy Impact Assessment Tool (D22-7264).

The *APS Privacy Governance Code* requires agencies subject to the Privacy Act to publish their PIA register. The Commission publishes its PIA register on its website at https://www.safetyandquality.gov.au/about-us/governance/privacy-impact-assessment-register.

## Roles and responsibilities

All Commission employees and contractors are responsible for ensuring that the Commission complies with privacy obligations by following the requirements under this Privacy Policy.

In accordance with the *Privacy (Australian Government Agencies – Governance) APP Code 2017*, the Commission has appointed a Privacy Champion to act as the Chief Privacy Officer and Privacy Officers. The Chief Privacy Officer is a senior official within the agency who is responsible for leadership activities and engagement that require broad strategic oversight. Privacy Officers are the first point of contact for privacy matters within the agency and are responsible for day-to-day operational privacy activities.

The Commission's Chief Privacy Officer and Privacy Officers are as follows:

**Chief Privacy Officer**

Catherine Katz
Director
Intergovernment Relations
catherine.katz@safetyandquality.gov.au

[2] https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response

**Privacy Officers**

Stan Ahn
Compliance & Procurement Manager
stan.ahn@safetyandquality.gov.au

Lauren Caleo
Senior Project Officer
National Standards
lauren.caleo@safetyandquality.gov.au

Katherine Norden
Senior Project Officer
Strategy and Innovation
katherine.norden@safetyandquality.gov.au

Damen Pearce (ICT matters)
Operations Manager
eHealth and Medication Safety
damen.pearce@safetyandquality.gov.au

## Access to personal information

Individuals can request access to their personal information held by the Commission. They can also request the Commission to correct their personal information if it is incorrect.

A person subscribed to one of the Commission's distributions such as *On the Radar* can opt out by using the unsubscribe option included in the distribution.

To contact the Commission regarding any privacy inquiry or complaint, or to request for access to your personal information, please contact the Commission on +61 2 9126 3600 or write to GPO Box 5480 Sydney, NSW, 2001 addressed to the Chief Privacy Officer or a Privacy Officer.

## Australian Privacy Principles

The APPs were released by the OAIC and came into effect on 12 March 2014. The APPs include 13 principles that outline how Australian organisations should handle, use and manage personal information.

The Commission's treatment of, and compliance with, the 13 APPs are outlined in **Appendix 1**.

**Appendix 1 – Treatment of, and compliance with, the Australian Privacy Principles (APP)**

| Australian Privacy Principle (APP) | Requirement | Treatment | Compliant? |
|---|---|---|---|
| **Consideration of privacy of personal information** | | | |
| APP1 – Open and transparent management of personal information | Manage personal information in an open and transparent way. This includes having a clearly expressed and up-to-date Privacy Policy which is available to the public. | The Commission discloses purposes of collecting personal information.<br><br>The Commission uploads its Privacy Policy on its website. | Yes |
| APP 2 – Anonymity and pseudonymity | Provide individuals with the option of not identifying themselves, or of using a pseudonym. Some exceptions can apply. These include where the Commission is required or authorised by or under an Australian law to deal with individuals who have identified themselves; or it is impracticable for the Commission to deal with individuals who have not identified themselves. | Where personal information is being requested for purposes other than administrative functions (such as payroll), disclosure of such personal information is requested on voluntary basis. | Yes |
| **Collection of information** | | | |
| APP3 – Collection of solicited personal and sensitive information | Do not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the Commission's functions or activities. The Commission must not collect sensitive information about an individual unless the individual has consented to the collection of the information and the information is | The Commission collects personal information that is reasonably necessary for, or directly related to, one or more of its functions or activities. These include information collected for the purposes of payroll, payment of reimbursement or sitting fees, appointment of individuals to | Yes |

| | | | |
|---|---|---|---|
| | reasonably necessary for, or directly related to, one or more of the Commission functions or activities. Under the exceptions listed in APP3.4, the Commission can solicit sensitive information in some cases without complying with APP3.3 if the collection is required or authorised by or under an Australian law. The Commission must collect personal information about an individual only from the individual unless the individual consents to the collection of the information from someone other than the individual, or the Commission is required or authorised by or under an Australian law to collect the information from someone other than the individual or it is unreasonable or impracticable to do so. | committees and other similar functions.<br><br>The Commission requests personal information directly from the individual. | |
| APP4 – Dealing with unsolicited personal information | If the Commission receives unsolicited personal information, the Commission must determine whether it could have obtained the information under APP3 if the Commission had solicited the information. If the Commission determines that it could not have collected the information and the information is not contained in a Commonwealth record, the Commission must destroy the information or ensure that the information is de-identified but only if it lawful and reasonable to do so. | The Commission appropriately deals with unsolicited personal information including expunging unsolicited personal information from the Commission's records management system unless required to retain the information by Australian law. | Yes |
| APP5 – Notification of the collection of personal information | The Commission must, either at or before the collection of personal information, notify individuals on the purpose of collecting the personal information; requirements for | The Commission advises the purpose of collecting personal information and ramifications associated with being unable to collect the information. | Yes |

| | | | |
|---|---|---|---|
| | accessing the information, ramifications of failure by the Commission to collect the information and whether the information is required under Australian law or a tribunal/court order. | | |
| **Dealing with personal information** | | | |
| APP6 – Use and disclosure of personal information | Only use the personal information collected for its primary purpose unless the individual has consented to the use or disclosure for a secondary purpose, or if the exceptions apply in APP6.2 or 6.3. These exceptions include whether the individual would reasonably expect the Commission to use the information for the secondary purpose and where disclosure is required by the Commission to use or disclose the information for a secondary purpose which is directly related to the primary purpose. | The Commission uses personal information only for the purpose for which it has been collected. | Yes |
| APP7 – Direct Marketing | Do not use or disclose personal information for the purpose of direct marketing. | The Commission does not engage in direct marketing activities. | N/A |
| APP8 – Cross-border disclosure of personal information | Before the Commission discloses personal information about an individual to an overseas recipient, it must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs, other than APP1, in relation to the information. | The Commission undertakes its due diligence by assessing risks associated with sending personal information overseas prior to doing so. | Yes |
| APP9 – Adoption, use and disclosure of government | Do not adopt, use or disclose government | This APP applies to non-government | N/A |

| | | | |
|---|---|---|---|
| related identifier | related identifiers. | entities only. | |
| **Integrity of personal information** | | | |
| APP10 – Quality of personal information | Take such steps (if any) as are reasonable in the circumstances to ensure personal information that is collected, used or disclosed is accurate, current, complete and relevant. | The Commission undertakes steps that are reasonable to ensure personal information required for the purposes of its administrative functions is accurate, current, complete and relevant. | Yes |
| APP11 – Security of personal information | Take such steps as are reasonable in the circumstances to ensure that personal information is protected from misuse, interference, loss and from unauthorised access, modification or disclosure. The Commission must also take reasonable steps to destroy or de-identify personal information if it is no longer needed for any purpose for which it may be used or disclosed, so long as the information is not contained in another Commonwealth record and the Commission is not required under an Australian law to retain it. | All Commission information, regardless of whether it is personal information, is stored in the Electronic Document and Records Management System (EDRMS) provided by the Australian Government Department of Health. The Commission receives regular assurances from Health IT that its IT environment, including the EDRMS, is secure. | Yes |
| **Access to, and correction of, personal information** | | | |
| APP12 – Access to personal information | Give an individual access to their personal information upon request of that individual. The Commission can refuse to give access to the information under the Freedom of Information Act 1982 or any other Commonwealth Act, to the extent that the Commission is required or authorised to refuse access. The Commission must respond to the request for information and | The Commission provides an individual access to their personal information upon request.<br><br>The Commission's Privacy Policy includes contact details for the Commission's Privacy Champion and Privacy Officers in the event an individual wishes to lodge a complaint | Yes |

| | | | |
|---|---|---|---|
| | give access to the information if it is reasonable and practicable to do so. Where an individual's request for information is refused, the Commission must give reasons to the individual for that refusal and mechanisms available to complain about the refusal, unless it would be unreasonable to do so. | regarding the Commission's treatment of their privacy or personal information. | |
| APP13 – Correction of personal information | Take reasonable steps to correct personal information that the Commission holds when the information is inaccurate, out-of-date, incomplete, irrelevant, misleading or where the individual requests the Commission to correct the information. Where personal information is corrected, the Commission must take reasonable steps to notify third parties of the amendment. | The Commission undertakes steps that are reasonable to ensure that the personal information that it collects is accurate. | Yes |