



Australian
Commission on
Safety and Quality
in Health Care

D14-15168

Privacy Policy

30 November 2024
1.10

Document Control

Version History

Version	Issue date	Author	Reviewers	Outcome of review
v0.1	May 2014	Jason Whatley	Mike Wallace, Chief Operating Officer	Drafted
v0.11	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 Board	Endorsed Approved on 7 August 2014
v1.01	May 2017	Stan Ahn	Mike Wallace, Chief Operating Officer	Annual review
v1.02	Feb 2018	Stan Ahn Lisa Murphy Damen Pearce	Catherine Katz, Chief Privacy Officer Mike Wallace, Chief Operating Officer	Included the Commission's privacy framework and added the Commission's management of the Notifiable Data Breaches Scheme. Approved at the 21 February 2018 meeting.
v1.03	Dec 2018	Stan Ahn		Included D Pearce as one of the privacy officers.
v1.04	Mar 2019	Stan Ahn	 Catherine Katz, Chief Privacy Officer Mike Wallace, Chief Operating Officer	Included a new paragraph on joint notifiable data breaches. Included a new section on the Commission's Privacy Management Plan. Approved Approved

v1.05	Feb 2021	Stan Ahn		Periodic review. Minor typographical corrections and updates to hyperlinks.
v1.06	Oct 2021	Stan Ahn		Updated Document Ownership Details with Chris Leahy as the COO.
v1.07	Mar 2022	Stan Ahn	Catherine Katz, Chief Privacy Officer Chris Leahy, Chief Operating Officer	Included process for conducting Privacy Impact Assessments. Approved Approved
v1.08	Apr 2023	Stan Ahn		Updated the Commission's Privacy Officers.
v1.09	Feb 2024	Allan Moore		Minor typographical update Updated the Commission's Privacy Officers.
v1.10	Nov 2024	Stan Ahn	Catherine Katz, Chief Privacy Officer Naomi Poole, A/g Chief Operating Officer	Included the Privacy Disclaimer template as Appendix 1. Included Meeting Recording rules as Appendix 2. Other typographical updates. Approved Approved

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 plan will be reviewed annually or as required.

Table of contents

Version History	2
Ownership	4
Glossary	6
Introduction	7
Privacy Framework	7
Resources	8
Scope	8
Purpose	8
Definition of 'personal information'	8
Type of information collected by the Commission	9
Collecting and holding personal information	10
Using personal information	10
Disclosure of personal information	11
Quality and security of personal information	11
Privacy or data breach	12
Privacy Management Plan	14
Roles and responsibilities	14
Access to personal information	15
Australian Privacy Principles	15
Appendix 1 – Privacy disclaimer and template	16
Appendix 2 – Treating meeting recordings	17
Appendix 3 – Treatment of, and compliance with, the Australian Privacy Principles (APP)	19

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: information collected in connection with the provision of a health service information or opinion about the health or disability of an individual an individual’s expressed wishes about the provision of health services any information about health services provided to an individual
NDB	means Notifiable Data Breaches
NDB scheme	means the <i>Privacy Amendment (Notifiable Data Breaches) Act 2017</i> which came into effect from 22 February 2018 and introduced 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 <i>National Health Reform Act 2011</i>
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 <i>Privacy Act 1988</i>
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, the state and territory privacy laws and healthcare regulations and the Commission's formal agreements for accessing healthcare information..

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 (including 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.

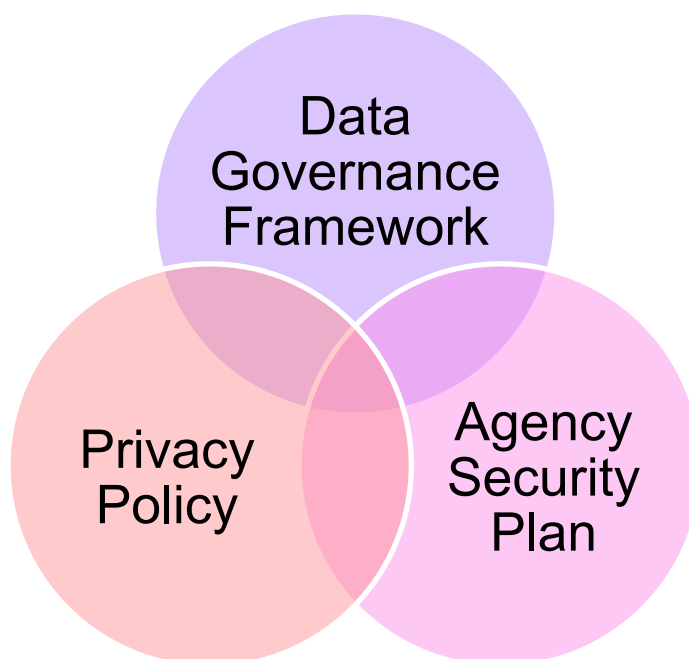


Figure 1 - Commission's privacy framework

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 apply 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

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

‘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 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 after obtaining consent, unless it is unreasonable or impracticable to collect that information from the person, or the Commission is required or authorised to collect the information 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 about:

- the purpose for collecting the information
- the Commission's requirements to access the information
- how the information will be stored
- ramifications if the Commission is unable to collect the information
- whether the information is required under Australian law.

The Commission's template for providing such a privacy statement is at **Appendix 1**.

Recordings of a meeting

The definition of personal information in the Privacy Act includes information or an opinion from an individual. During a meeting, attendees may potentially express their opinions or views, which must then be treated under this Policy.

Additional information in relation to creation and use of meeting recordings is outlined in **Appendix 2**.

Unsolicited personal information

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.

Records management

The Commission uses TRIM as its official electronic records management system for storing 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 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 about committee members to establish and maintain its 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 members' bank accounts, taxation and superannuation details in order to act as an employer and pay sitting fees.

Personnel files

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

Personal information collected through consultation

The Commission routinely collects information through consultation and feedback across program areas. This can include:

- written submissions
- an online survey platform
- minutes or recordings of meetings.

Information collected may include names, email addresses, phone numbers, details of workplaces and opinions. Personal information which is not already in public domain is de-identified for external use and is treated in line with this Policy.

Corporate information

Additionally, the Commission collects and uses corporate information that may contain information relating to a person in their corporate capacity, such as corporate contact details and job titles.

Corporate information does not meet the definition of personal information under the Privacy Act. If a person's corporate information is considered sensitive, the Commission treats such information as commercial-in-confidence if.

Disclosure of personal information

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

The Commission discloses personal information to other organisations including 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 and Aged Care payroll.

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.

Quality and security of personal information

The Commission applies the principles set out in the Australian Government Protective Security Policy Framework (PSPF) and Australian Government Information Security Manual (ISM) for protecting 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'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 introduced 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 2 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.

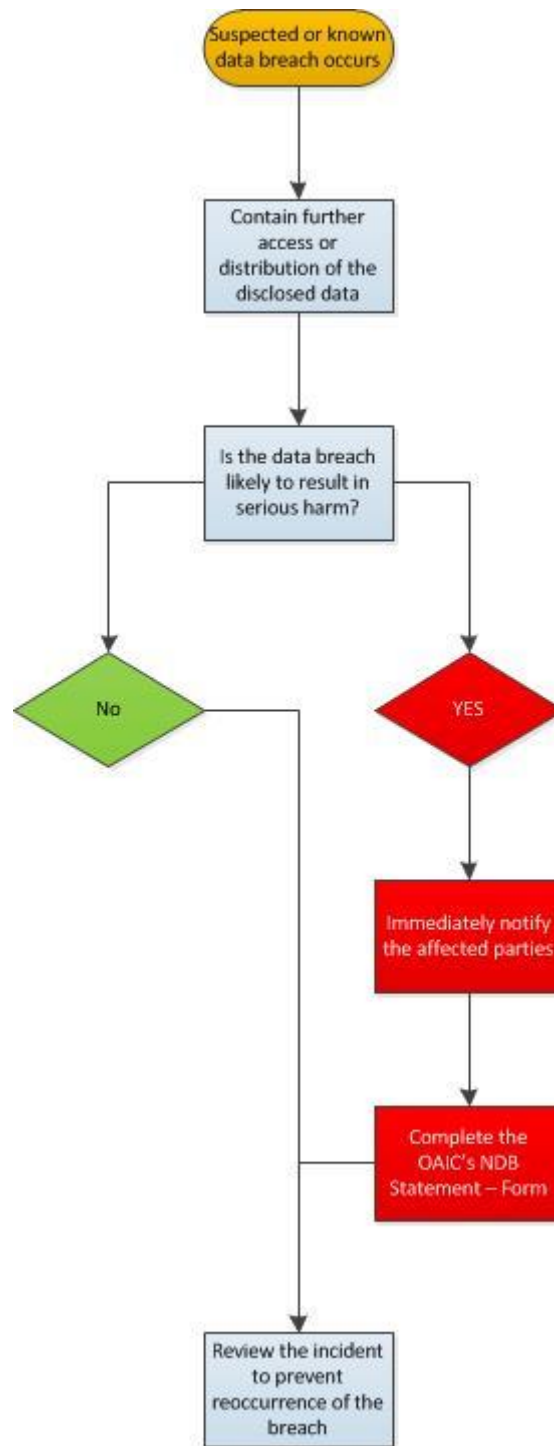


Figure 2 - Commission's process for the NDB scheme

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

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

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

Privacy Officers

Stan Ahn
Director, Business Unit
stan.ahn@safetyandquality.gov.au

Vanessa Cooper
Senior Project Officer

Safety and Quality Improvement Systems
vanessa.cooper@safetyandquality.gov.au

Katherine Norden-Ash
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

Allan Moore
Compliance and Procurement Manager
allan.moore@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 3**.

Appendix 1 – Privacy disclaimer and template

Advice to staff

The Australian Commission on Safety and Quality in Health Care (the Commission) collects personal information when it is reasonably necessary for, or directly related to, the Commission's functions or activities.

To comply with the requirements of the Australian Privacy Principle 5 (notification of the collection of personal information) under the *Privacy Act 1988*, the Commission must, either at or before the collection of personal information, notify individuals of the following:

- purpose of collecting the personal information
- requirements for accessing the information
- ramifications of failure by the Commission to collect the information
- if applicable, that the information is required under Australian law or a tribunal/court order.

When undertaking activities that require collecting personal information, staff must use the disclaimer below.

Privacy Disclaimer

The Australian Commission on Safety and Quality in Health Care (the Commission) collects personal information when the information is necessary for, or directly related to, the Commission's functions or activities.

Your personal information is being requested by the Commission to fulfil its **function as an employer/purpose under legislation [delete whichever is not applicable]**. Your personal information will be used to **[insert details of the requirements for accessing the information, for example, "contact you to seek clarification on the feedback you provided in your survey/undertake recruitment and selection process/administer your committee membership"]**.

If you do not provide the requested personal information, the Commission may not **[insert details of ramification, e.g. "consider your feedback obtained during the consultation phase/process your application further for the recruitment /pay or administer your sitting fees and travel"]**.

All personal information is held securely. The Commission treats all personal information in accordance with the Australian Privacy Principles under the *Privacy Act 1988* (the Act) and the Commission's Privacy Policy. The Commission does not disclose personal information to other organisations unless it is required to do so under the Australian law or tribunal/court order. The Commission's Privacy Policy is available from the Commission's website at www.safetyandquality.gov.au.

Appendix 2 – Treating meeting recordings

The Commission may record its meetings for various official purposes. These purposes can range from developing more accurate meeting minutes to circulating the recordings to absent participants.

Under the shared services arrangement with the Australian Government Department of Health and Aged Care, the Commission uses Microsoft Teams (MS Teams) to conduct videoconferences. MS Teams includes ‘quality of life’ functions for easily sharing meeting recordings. Such recordings must be handled with care and in ways that meet the Commission’s privacy obligations.

Rules

Commission staff must follow the following rules for meeting recordings:

1. The intended purpose for the recording must be established prior to the meeting.
2. Whenever possible, active consent must be sought prior to, or at the commencement of, a meeting.
3. Meeting recordings must only be distributed to the intended recipients.
4. Meeting recordings must be protected appropriately within TRIM.

Meeting recordings in this policy refer to both video and audio recordings and their transcripts.

1. Establish the intended purpose

The Commission adheres to the privacy principle that information must only be used for the purpose for which it has been collected. Prior to recording a meeting, the purpose for the recording must be established. This purpose must be advised to the meeting participants when seeking their consent to record the meeting (see Step 2).

The meeting recording should only be used for the established purpose. The purpose for the meeting recording should not change once it has been established. For example, it is not appropriate to advise the participants that the meeting recording will be used for the purpose of developing meeting minutes, then circulate the recordings or use them for a purpose that is different to what was advised to the participants.

2. Active consent versus passive consent

Active consent means participants expressly consent to be recorded. For example, asking meeting attendees to raise their hands if they consent to be recorded is a form of active consent.

Passive consent means a lack of objection is taken to mean that they consent to be recorded. For example, advising attendees that they agree to be recorded by participating in the meeting is a form of a passive consent.

It is better practice to seek active consent from participants rather than accepting a lack of objection as an implied, passive consent. However, in situations where seeking active consent is not possible or difficult due to the size and composition of the meeting, it is acceptable to proceed with passive consent.

Consent can be sought either prior to the meeting, such as in the meeting invitation, or at the beginning of the meeting. When seeking consent, the following information should be provided to the participants:

- Intended purpose of recording the meeting.

- That participants can request a copy of the recording.
- Ramifications if they do not agree to the meeting being recorded, or do not agree to be included in the recording.
- Ramifications if the Commission is not able to record the meeting.

Example consent statement

Below is an example consent statement which can be included in a meeting invitation. The statement is an example only and should be adjusted as appropriate depending on the meeting circumstance.

The Commission would like to record this meeting for the purpose of distributing the recording to participants who are an apology for this meeting. Once recorded, the recording will form an official record of the meeting in addition to the meeting minutes. Those who are present can also request a copy of the recording.

The Commission requires participants to consent to be included in the recording. If you do not wish to be included in the recording, please advise via a reply email. If you do not consent to be recorded, please note that, while you can attend the meeting, [you will not be able to participate in the discussions/the Commission will not record the meeting].

3. Distributing a meeting recording

If the recording purpose includes distribution, the meeting recording can only be distributed to the intended recipients. The intended recipients must be identified when establishing the purpose of the recording. It is not acceptable to change the intended recipients after a recording has already been made. For example, it is not appropriate to obtain consent from the participants to record a meeting by advising that the meeting recording will be distributed to the meeting attendees and apologies, then circulate the recording to other external individuals.

4. Protecting the meeting recording

Meeting recordings must be kept in TRIM and should not be stored outside the Commission's record management systems such as personal devices. If personal or sensitive information is discussed in the meeting, appropriate access control must be applied to the recording file to ensure that only those with the need-to-know basis can access the recording. If the purpose of the recording is time-limited such as using it as a reference for developing minutes, the recording should be deleted from TRIM once its purpose has been achieved.

Appendix 3 – 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. 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 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	Yes

	<p>the information and the information is 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.</p>	<p>fees, appointment of individuals to committees and other similar functions. The Commission requests personal information directly from the individual.</p>	
<p>APP4 – Dealing with unsolicited personal information</p>	<p>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.</p>	<p>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.</p>	<p>Yes</p>
<p>APP5 – Notification of the collection of personal information</p>	<p>The Commission must, either at or before the collection of personal information, notify individuals on the purpose of collecting the personal information; requirements for accessing the information, ramifications of failure by the Commission to collect the</p>	<p>The Commission advises the purpose of collecting personal information and ramifications associated with being unable to collect the information.</p>	<p>Yes</p>

	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 related identifier	Do not adopt, use or disclose government related identifiers.	This APP applies to non-government entities only.	N/A
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 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	The Commission provides an individual access to their personal information upon request. 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 regarding the Commission's treatment of their privacy or personal information.	Yes

	complain about the refusal, unless it would be unreasonable to do so.		
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