



Australian Government

Professional Services Review

PSR Privacy Policy

1. Introduction

As an Australian Government agency the Professional Services Review (PSR) operates subject to the [Privacy Act 1988](#) (the Privacy Act) and in particular the [Australian Privacy Principles](#) (APPs) found in that Act. The Privacy Act and the APPs outline the specific legal obligations of PSR when collecting and handling your personal information.

The Privacy Act requires entities bound by the APPs such as PSR, to have an APP Privacy Policy.

An APP Privacy Policy is defined as a clearly expressed and up to date policy regarding an APP entity's management of personal information. This Privacy Policy outlines the personal information handling practices of the PSR. We will update this Privacy Policy when our information handling practices change. Updates will be published on our website.

2. About PSR

PSR is a small agency within the Commonwealth Health portfolio. PSR is responsible for providing administrative support and legal services to the Director of PSR, PSR peer review Committees and the Determining Authority in performing their respective functions under Part VAA of the [Health Insurance Act 1973](#). Further information about PSR can be found on PSR's [website](#).

3. The Privacy Act

The Privacy Act regulates how APP entities such as PSR collect, hold, use and disclose 'personal information' which is a defined term in the Act. The Privacy Act also provides for individuals to seek access to, and correction of, their personal information.

Personal information is information or opinion in any form that identifies, or enables identification of, a living person. The complete definition in the Privacy Act is:

'Personal Information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- (a) *whether the information or opinion is true or not; and*
(b) *whether the information or opinion is recorded in a material form or not.'*

Personal information includes information such as:

- your name or address
- bank account details and credit card information
- photos
- internet clickstream
- cookies data; or
- information about your opinions.

The thirteen APPs in Schedule 1 of the Privacy Act regulate how agencies (including PSR) can:

- collect
- use
- disclose
- store; or
- access

your personal information.

PSR is required to comply with the Privacy Act and, in particular, the thirteen APPs which regulate the collection, storage, use and disclosure of personal information.

4. PSR's Personal Information Handling Practices

4.1 Collection of personal information generally

PSR only collects personal information in accordance with the APPs. PSR collects personal information it needs in order to perform its functions and activities under the *Health Insurance Act 1973*. PSR collects personal information through a range of different channels including:

- paper-based and electronic forms (including online forms)
- face to face meetings
- telephone, email, videoconference and facsimile communications
- from persons under review and third parties under Notices issued pursuant to section 89B and section 105A of the Act
- PSR's secure online file sharing platform software, Kiteworks; and
- PSR's website.

PSR only collects personal information in a limited range of categories. These categories include:

- information about medical and other health practitioners when Medicare requests PSR to review their provision of services under the Medicare or Dental Benefits Programs or the Pharmaceutical Benefits Scheme

- personal information about individuals who have received services under the Medicare and dental benefits programs and the Pharmaceutical Benefits Scheme from or on behalf of practitioners who are the subject of a review by PSR
- personal information collected by contracted service providers in compliance with contractual measures as required by the Privacy Act
- personal information collected from employees, job applicants, contractors and others in relation to employment at PSR (e.g. personnel records, health information, email and telephone records, and information on work related travel or other expenses)
- documents relating to appointments of persons to the PSR Panel and Determining Authority
- personal information to facilitate the operation of PSR's secure online file sharing platform, Kiteworks
- information relating to work health and safety assessments, incidents and investigations
- financial and other information about tenderers, contractors and customers
- tax file number (TFN) information
- distribution and mailing lists; and
- contact lists.

The APPs provide that PSR may only collect information for a lawful purpose that is directly related to a function or activity of PSR and when the collection is necessary for, or directly related to, that purpose. For example, PSR collects personal information to enable us to:

- administer the PSR Scheme under the *Health Insurance Act 1973*
- administer relevant superannuation benefits
- manage employees, including to ensure or promote the health and safety of all employees
- process work related expenses for PSR Panel members and members of the Determining Authority (for example corporate travel and other related expenses); and
- manage appointments to the PSR Panel and Determining Authority.

4.2 Privacy notice

PSR routinely provides a privacy notice as required by APP 5 when it solicits personal information. While PSR is not routinely required to provide a notice under APP 5 to individuals who have received services from a person under review, how PSR handles personal information is addressed in this policy.

Occasionally, we may receive and collect personal information about you from you, individuals or other entities, without it being requested by us. This information is considered 'unsolicited'. PSR does not normally give an APP 5 privacy notice in these circumstances because of the unsolicited nature of the information received.

In all cases where personal information is received, it is handled according to the particular circumstances and in compliance with the Privacy Act.

4.3 Kinds of personal information collected and held

Personal information PSR collects and holds may include:

- name, address and contact details (e.g. phone, email and fax)
- date of birth
- gender
- government identifiers (e.g. Medicare number)
- curriculum vitae
- qualifications and referee reports
- signature
- driver's licence and passport information
- travel booking details
- bank account and superannuation details and other financial information; or
- next of kin.

4.4 Sensitive Information

Where the above kinds of personal information include sensitive information such as:

- racial or ethnic origin
- criminal record
- health information such as details of an individual's medical history, including details of specific medical conditions, disabilities and medication history including where relevant to the management of your health and safety or the health and safety of all employees
- information relevant to a work health and safety assessment, incident or investigation; or
- information about an individual's membership of a professional association,

this information is given the higher level of protection required by the APPs.

If you or another person provides PSR with sensitive information, PSR will only retain the information if:

- you have consented to the collection of the information and it is reasonably necessary for, or directly related to, one of PSR's functions or activities
- collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or
- collection of the information is authorised for other purposes permitted under the Privacy Act – this includes where PSR:
 - suspects that unlawful activity, or serious misconduct, relating to PSR's functions and activities has been, is being or may be engaged in; or
 - reasonably believes that the collection is necessary to lessen or prevent a serious threat to the health or safety of any individual, or to public health or safety.

If the sensitive information does not fall within one of these categories, PSR will not keep a record of the information and instead we will arrange for its return or secure destruction if it is lawful and reasonable to do so.

4.5 TFN Information

A TFN is a unique identifier issued by the Commissioner of Taxation. PSR may collect TFN information from individuals and employees for the purpose of carrying out its functions and activities.

Pursuant to sub-rule 8(2) of the *Privacy (Tax File Number) Rule 2015*, when collecting TFN information, PSR will notify you:

- of the taxation law, personal assistance law or superannuation law which authorises PSR to request or collect the TFN
- of the purpose(s) for which the TFN is requested or collected
- that declining to quote a TFN is not an offence; and
- of the consequence of declining to quote a TFN.

4.6 Use and disclosure of personal information

Use of personal information for primary purpose

PSR may use and disclose collected personal information for the primary purpose for which it was collected, including to:

- respond to correspondence
- provide secretariat services
- manage appointment processes to the PSR Panel and Determining Authority;
- maintain contact with stakeholders, and other Government agencies
- carry out ordinary government functions and activities such as briefing Ministers, responding to parliamentary questions and inquiries
- manage human resources and manage finances, including corporate travel and expenses for employees of PSR and PSR Panel Members and members of the Determining Authority
- manage PSR's workforce and assist in complying with PSR's workplace health and safety obligations;
- facilitate the sharing of information on PSR's secure online file-sharing platform, Kiteworks; and
- perform PSR's other functions in accordance with the *Health Insurance Act 1973*.

Under the Privacy Act we are required to take contractual measures to ensure that contracted service providers (including subcontractors) comply with the same privacy requirements applicable to us.

Use of personal information for secondary purpose

PSR may also use or disclose your personal information for a secondary purpose where an exception applies. Exceptions include:

- an individual has consented to a secondary use or disclosure

- an 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
- the secondary use or disclosure of the personal information 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 of the personal information – this includes where PSR
 - suspects that unlawful activity, or serious misconduct, relating to PSR’s functions and activities has been, is being or may be engaged in, or
 - reasonably believes that the further use is necessary to lessen or prevent a serious threat to the health or safety of any individual, or to the public health or safety; or
- PSR 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 believes that the collection is necessary to lessen or prevent a serious threat to the health or safety of any individual, or to public health or safety.

Disclosure of personal information to the Department of Finance and other third parties

PSR may also disclose your personal information to the Department of Finance who manage a cloud based information storage and sharing system (see paragraph 4.9 of this policy for more detail). This information may be disclosed to an overseas recipient for the primary purpose for which it was collected, consistent with performance of PSR’s functions under the *Health Insurance Act 1973*. Your personal information may, for example, be hosted on servers in Singapore or Hong Kong.

Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs

Your personal information will (where relevant) be handled in accordance with the *National Health (Privacy) Rules 2021* made under section 135AA of the *National Health Act 1953*.

Destruction of personal information

We will take reasonable steps to destroy or de-identify your personal information if we no longer need it for the purpose it was collected, unless it is contained in a Commonwealth record or we are required by law to retain the information.

4.7 How to seek access to and correction of personal information

Access to your personal information under the Privacy Act

PSR takes steps to ensure that the personal information we collect is accurate, up to date and complete. These steps include maintaining and updating personal information when we are advised by individuals that their personal information has changed, and at other times as necessary.

Under the Privacy Act an individual has a right to ask for access to personal information that PSR holds and ask that we correct that personal information. You can ask for access or correction by contacting us using the contact details set out at paragraph 6 of this APP Privacy Policy. PSR must respond to your request within 30 days. If you ask, we must give you access to your personal information, and take responsible steps to correct it if we consider it is incorrect, unless there is a law that allows or requires us not to.

Access to your personal information under the Freedom of Information Act 1982 (FOI Act)

Alternatively, you may make a request for access to documents containing your personal information under the FOI Act, by emailing PSR's FOI Coordinator at foi@psr.gov.au. Under the FOI Act, PSR is entitled to refuse access or only give access to certain information (for example, where the personal information is contained within a document that is commercially sensitive). If PSR denies an FOI request, in whole or in part, PSR will set out its reasons in writing.

PSR will try to make personal information available within 30 days after receiving an individual's request. There is no charge for PSR providing the individual's personal information under a request or under the FOI Act. However, some charges may apply to requests under the FOI Act that extend to additional documents.

Further information about making FOI requests (including when fees and charges may apply) is available on PSR's [FOI web page](#) or by telephoning (02) 6120 9100.

Updating your personal information

It is important to tell us if circumstances change to ensure that the information we hold, use or disclose about you is accurate, up-to-date and complete. You can contact us to update your personal information using the contact details set out at the end of this Privacy Policy.

4.8 Storage and Security

Personal information may be held by us or by people or organisations (including contracted service providers) acting on our behalf.

PSR has controls in place to protect the information we collect from loss, unauthorised access or disclosure and from any other misuse. Our controls include:

- access to personal information collected is restricted to authorised persons
- our internal network and databases are protected using firewall, intrusion detection and other technologies and can only be accessed by authorised users
- paper files containing personal and sensitive information are protected in accordance with Australian Government security policy
- PSR's premises are under 24-hour surveillance and access is via security passes only, with all access and attempted access logged electronically; and

- PSR conducts system audits and staff training to ensure adherence to our established protective and IT security practices.

PSR stores and disposes of personal information in accordance with the *Archives Act 1983*.

4.9 Cloud based storage

GovTeams

PSR makes use of GovTEAMS, an online workspace for whole of government collaboration, to temporarily store personal information. GovTEAMS is managed by the Department of Finance (and provided by a third-party). In order to protect personal information once it leaves the PSR environment for the cloud computing environment, the Department of Finance:

- ensures that its cloud service providers are contractually bound to protect personal information in accordance with the Privacy Act
- ensures cloud service providers offer personal information security measures that are at least equal to those used by the Department of Finance; and
- ensures contractual arrangements are in place with cloud service providers to destroy or de-identify personal information once it is no longer needed.

Finance's use of cloud computing environments is informed by the following document: [Commonwealth of Australia \(Digital Transformation Agency\) *Secure Cloud Strategy*](#).

Kiteworks

Personal information (e.g. a person's name and email address) is used to facilitate the operation of PSR's secure online file sharing platform, Kiteworks. User activity in Kiteworks is logged and may be used to review user access and actions, for business administration and security purposes.

PSR uses Kiteworks to facilitate the legitimate sharing of personal information with relevant parties during the PSR review process and to conduct PSR agency operations. This requires PSR to temporarily store personal information in Kiteworks' cloud based storage. At the conclusion of a matter, all related information is permanently deleted from Kiteworks.

In order to protect personal information shared using Kiteworks and stored in the cloud:

- the platform is Infosec Registered Assessor Program (IRAP) certified and hosted in Australia in an IRAP compliant data centre
- PSR has its own Kiteworks tenancy where the PSR data is stored in an encrypted form; and
- all data in transit to and from the system is encrypted (https-protocol).

PSR also makes use of the Australian Health Practitioner Regulation Agency's (AHPRA) Kiteworks platform.

4.10 Cookies, Google Analytics and Clickstream data

When you visit the PSR website, we use Google Analytics to collect or view website traffic information. Google Analytics has their own privacy policy. Information collected when you visit the PSR website may include the IP address of the device you are using and information about sites that IP address has come from. PSR uses this information to maintain and improve our website. In relation to Google Analytics, you can opt out of the collection of this information using the Google Analytics Opt-out Browser Add-on.

4.11 Privacy Impact Assessments

PSR is required to conduct a Privacy Impact Assessment (**PIA**) for all high risk privacy projects.

The *Privacy (Australian Government Agencies – Governance) APP Code 2017* provides that a project may be a high risk privacy project if the agency reasonably considers that the project involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals.

A PIA is an assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. PSR publishes its register of completed PIAs on its [website](#).

5. Complaints

Complaints to PSR

If an individual believes PSR has breached his or her privacy rights, he or she may contact PSR using the contact details set out at paragraph 6 of this APP Privacy Policy. PSR will treat the complaint seriously and is committed to providing a fair and timely response. Please allow an adequate opportunity for the complaint to be dealt with by PSR, generally giving 30 days for a response.

Upon receipt of your complaint, PSR will:

- gather the facts relevant to the complaint
- investigate the issues raised and consider how your request regarding outcomes can be met
- communicate our response to you in person and in writing, and invite you to reply to our response
- identify any systemic issues raised and possible responses; and
- record your complaint and outcome.

These steps will be taken in accordance with the Office of the Australian Information Commissioner (**OAIC**) [checklist for addressing privacy complaints](#).

Complaints to the OAIC

If you are not satisfied with PSR's response to your complaint you may make a complaint to the OAIC. Where appropriate the OAIC can make preliminary enquiries into the matter, investigate and/or attempt to resolve the complaint by conciliation

More information about the [Commissioner's privacy complaint handling process](#).

The Australian Information Commissioner's details are set out below:

Telephone: 1300 363 992

Email: enquiries@oaic.gov.au

Post: Australian Information Commissioner

Office of the Australian Information Commissioner

GPO Box 5218

Sydney NSW 2001

6. How to contact PSR

Contact PSR's Privacy Officer if you want to:

- obtain access to your personal information
- request a correction to your personal information
- update your personal information
- make a complaint about a breach of your privacy
- query how your personal information is collected, used or disclosed
- make a suggestion or comment in relation to our Privacy Policy; or
- ask questions about our Privacy Policy.

PSR's Privacy Officer can be contacted by telephone on (02) 6120 9100 or by email at enquiries@psr.gov.au

Current version created: March 2022

Next review date: March 2023 (or earlier if required)