



PrivateHealth.gov.au

PRIVACY IMPACT STATEMENT

FEBRUARY 2019

Contents

Privacy Impact Assessment	1
Role of OAIC	1
What is a Privacy Impact Assessment?	1
Threshold Assessment	1
Plan the PIA.	2
General Description	2
Describe the Project	3
Identify and consult with stakeholders	3
Map Information Flows	4
Privacy Impact Analysis and Compliance Check	5
Privacy impact analysis	5
Privacy Management—Addressing Risks	9
Recommendations	10

Privacy Impact Assessment

Role of OAIC

Note: The *Privacy Act 1988* (Privacy Act) gives the Information Commissioner (IC) a power to direct an agency to provide a Privacy Impact Assessment (PIA) to the Office of the IC (OAIC), if the IC considers that a proposed activity or function of the agency might have a significant impact on the privacy of individuals (s33D Privacy Act). This includes when the agency proposes to engage in a new activity or function, or substantively change an existing activity or function e.g., a substantive change to the system that delivers an existing function or activity.

What is a Privacy Impact Assessment?

A Privacy Impact Assessment (PIA) is a systemic assessment of a project that may have privacy implications. The term project includes:

- policy proposal
- new or amended legislation
- new or amended program, system or database
- new methods or procedures for service delivery or information handling
- changes to how information is stored.

The PIA identifies the impact that the project might have on the privacy of individuals and sets out recommendations for managing, minimising or eliminating adverse impacts. It will go beyond assessing the project's risk of non-compliance with privacy legislation and identify controls to mitigate the risk.

This PIA will also consider the broader privacy implications and risks, including whether the planned uses of personal information in the project will be acceptable to the community.

This PIA has been prepared with reference to the Commonwealth Ombudsman's Privacy Impact Assessment Guidelines (attached to the [Privacy Policy](#)).

PrivateHealth.gov.au

PrivateHealth.gov.au provides people interested in private health insurance a website that explains the workings of private health insurance in Australia and the ability to search for and compare policies from all **37** insurers. A bespoke content management system is used to collect information on policies from these insurers.

Threshold Assessment

Will any personal information be collected? If yes, record a brief description of the personal information that will be collected, used or disclosed (such as name, address, date of birth, health information etc.).

The following information will be collected as part of searching for policies:

- Medicare status
- state of residence
- number of adults and children in a household
- clinical conditions or treatments of importance to the user.

Additional information is needed if the user chooses to estimate the premium they will pay for selected policies:

- household income band
- age group
- Lifetime health cover loading.

In calculating a user's lifetime health cover loading, we collect:

- date of birth
- time spent overseas or in certain industries (military) or regions (Antarctica)
- periods where the user held private health insurance.

This information is not associated with any identifying data, such as names, email addresses or phone numbers and unless the user chooses to retain it for future visits to the website, it is destroyed at the end of the session.

Where a user elects to save the results of a search, no username/password will be required. A unique key, known only to the user, will be used to retrieve the data. Unless the user requests a response to feedback, any user email address used to send them information will not be recorded in the database.

Plan the PIA.

General Description

Name of Program: PrivateHealth.gov.au
Date: Existing and ongoing
Name of Section/Branch: Private Health Insurance
PIA Drafter: Michael Rochford (Human Solutions)
Email: hs@hs.com.au Phone: 03 6211 3211
Program Manager: David McGregor
Email David.McGregor@ombudsman.gov.au Phone: x735

Definition—Project: For the purpose of this document, the term project is intended to cover the full range of activities and initiatives that may have privacy implications including:

- policy proposals
- new or amended legislation, programs, activities, systems or databases
- new methods or procedures for service delivery or information handling
- changes to how information is stored.

Describe the Project

The Commonwealth Ombudsman manages the website **privatehealth.gov.au**. Website development and maintenance is provided by Human Solutions Pty Ltd.

PrivateHealth.gov.au provides people interested in private health insurance a website that explains the workings of private health insurance in Australia and the ability to search for and compare policies from all 37 insurers. A bespoke content management system is used to collect information on policies from these insurers.

In order to provide more accurate results for consumers who are searching for health insurance policies or to estimate their Lifetime Health Cover (LHC) loading, consumers may be asked to provide some personal information such as state of residence and income bracket. This information is deleted at the end of each session unless the user requests to save their search results.

Information security is managed through a Risk and Threat Analysis Plan and Project Risk Register. The website provides general advice only and users are advised through disclaimers that if they provide inaccurate information, the results may also be inaccurate.

A PIA needs a broad 'big picture' description of the project. It should be kept fairly brief.

Identify and consult with stakeholders

Key stakeholders for **privateHealth.gov.au** are:

- Commonwealth Ombudsman—project owner
- Department of Health—Legislation and regulations
- Private health insurers—providers of policy data
- General public—users of the site.

Given the nature of the project, the lack of personally identifiable information and the roles of the above participants no formal consultation with the stakeholders has been done. The Department, insurers and representatives of consumer groups have been provided the opportunity to provide general input through the Consumer Website Reference Group.

Provide key privacy elements

In order to provide more accurate results for consumers who are searching for health insurance policies, consumers may be asked to provide some personal non-identifying information. This information includes state of residence, number of people to be covered, Medicare eligibility status, and income bracket.

To estimate a person's LHC loading, they may be asked to provide their date of birth, and entry and exit dates from Australia.

This information is collected on a voluntary basis. Identifying information such as names, address, phone or email are not requested for policy search or LHC purposes.

The key privacy elements in the design and implementation of the project are:

- By default, all information collected from users is deleted after a session closes.
- Where a user elects to save the results of a search, no username/password will be required as a unique key, known only to the user, will be used to retrieve the data.
- Unless the user requests a response for feedback, any user email address used to send them information will not be recorded in the database.

Map Information Flows

Describe and map the project's personal information flows.

Verification

Not required

Collection

As detailed above, personal information will be collected to facilitate searching for policies, estimating premiums and calculating lifetime health cover loadings. All this data will be collected through the **privateHealth.gov.au** website.

Use

As detailed above

Disclosure

No other party will be given access to user information

Information quality

The quality of the data used to search for policies, estimating premiums and calculating loadings is the user's responsibility. If the information provided by the consumer is inaccurate, their search results or LHC estimates may be inaccurate – appropriate disclaimers are provided to advise users that the website provides general advice only.

The data describing the policies is the responsibility of the insurers.

The descriptive and explanatory information on the site is the responsibility of the Ombudsman's office.

Naturally, there are validation routines to ensure data is within accepted ranges.

Security

Security for the project is being managed under a Risk and Threat Analysis Plan and Project Risk Register.

Retention and destruction

The information collected on **privateHealth.gov.au** is already de-identified. Material is retained and destroyed in accordance with the *Archives Act 1983*.

Access and correction

A user will be asked to verify or update any stored data before it is used for further searches for policies, estimation of premiums or calculation of loadings.

Privacy Impact Analysis and Compliance Check

Privacy impact analysis

The privacy impact analysis should attempt to determine whether the project has acceptable privacy outcomes, or unacceptable privacy impacts.

PrivateHealth.gov.au will not have any direct or indirect impact on the privacy of users of the site. Should an unauthorised user obtain access to the database of saved search results, the information is de-identified and cannot be linked back to a specific individual.

Ensuring compliance

You will need to consider whether your project complies with each of the Australian Privacy Principles (APPs).

#	Description of the privacy principle <i>(These can be deleted from your final report if they're not relevant to your project)</i>	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
1	Principle 1 – Open and transparent management of personal information The agency must have a clearly expressed and up to date APP privacy policy about the management of personal information by the agency.	<i>No identifying information such as name, address, phone or email is retained on the site.</i>	<i>Complies</i>	
2	Principle 2 – Anonymity and pseudonymity Individuals must have the option of not identifying themselves, or of using a pseudonym, note exceptions to this rule apply.	<i>See above</i>	<i>Complies</i>	
3	Principle 3 – Collection of solicited personal information Limits apply to only collect information where the information is reasonably necessary for or directly related to one or more of the agency's functions or activities.	<i>Information only collected to perform searches for policies, estimate premiums or calculate loadings.</i>	<i>Complies</i>	

#	Description of the privacy principle <i>(These can be deleted from your final report if they're not relevant to your project)</i>	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
4	Principle 4 – Dealing with unsolicited personal information Determine whether or not the agency could have collected the information under APP 3. If not, where it is lawful and reasonable to do so destroy or de-identify the information.	<i>All information collected is essential to performing the tasks identified.</i>	<i>Complies</i>	
5	Principle 5 – Notification of the collection of personal information Inform the person what information you are collecting, the purpose or use of the information and how they may access or complain about the use of the information. Also inform them if the agency is likely to disclose the information to overseas recipients.	<i>Explanations on the site as to why information is required, how it is managed and that it is not disclosed to other parties.</i>	<i>Complies</i>	
6	Principle 6 – Use or disclosure of personal information Use it for the purpose you collected it for, unless one of the exceptions applies.	<i>Information is only used for the specified tasks and analysis of site usage patterns.</i>	<i>Complies</i>	
7	Principle 7 – Direct marketing Information not to be disclosed for the purpose of direct marketing unless exceptions apply, e.g., consent.	<i>N/A</i>	<i>Complies</i>	

#	Description of the privacy principle <i>(These can be deleted from your final report if they're not relevant to your project)</i>	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
	Principle 8 – Cross-border disclosure of personal information. Requirement to ensure overseas recipient does not breach APPs note exceptions apply e.g. information is subject to a law similar to APP's.	N/A	Complies	
9	Principle 9 – Adoption, use or disclosure of government related identifiers. Only assign unique identifiers where permitted. Agency should not disclose identifiers unless permitted.	N/A	Complies	
10	Principle 10 – Quality of personal information. Ensure information is accurate, up to date, complete and relevant prior to using it.	Users must confirm or update any stored data before it is used.	Complies	
11	Principle 11 – Security of personal information. Take care of the information and protect it against loss, modification, or unauthorised disclosure and other misuse. When no longer required either destroy or de-identify it.	All data is stored in a secure database. Where a user elects to save the results of a search, no username/password will be required as a unique key, known only to the user, will be used to retrieve the data. Email addresses will not be retained.	Complies	

#	Description of the privacy principle <i>(These can be deleted from your final report if they're not relevant to your project)</i>	Summary of personal information involved, use and process to manage	Assessment of compliance	Link to risk assessment (if required)
12	Principle 12 – Access to personal information People have a right to see their personal information noting exceptions apply, e.g. FOI exemptions.	N/A	Complies	
13	Principle 13 – Correction of personal information Agency must take steps to correct personal information held, ensure information is up to date, accurate, complete and not misleading.	N/A	Complies	
14	Other privacy interests	N/A	Complies	

Privacy Management—Addressing Risks

A risk is something that could lead to the unauthorised collection, use, disclosure or access to personal information.

Use the table below to list each of the privacy risks identified and the mitigation strategies/tools that will be implemented to mitigate these. Add extra rows as required. Please specify the likelihood of the risk arising, the degree of impact it would have on individual's privacy if it occurred and an assessment (low/medium/high) of the residual risk. It may be helpful to categorise these risks into areas such as: governance, people, process, technology.

Risk Mitigation Table					
	Identified Risk	Mitigation Strategy	Likelihood	Impact	Risk Rating
1	Database intruders downloads personal data	Data automatically de-identified Information security management plan in place	Low	Minor – no impact on any individual. However possible reputational impact for Ombudsman's Office.	Low

		and implemented			
		Project risk register updated regularly and steps taken to mitigate risk			

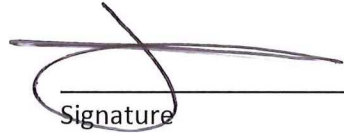
Recommendations

Summarise the recommendations to minimise the impact on privacy based on your risk assessment.

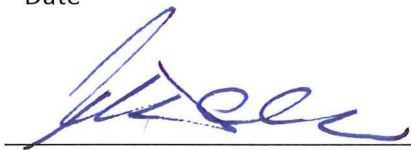
Ref	Recommendation	Agreed Y/N
R- 01	Appropriate security certification, system security plan, and security risk management plan implemented for website.	Y

Signatures

DERMOT WALSH
Name of Senior Assistant Ombudsman responsible


Signature

Date


Rodney Lee Walsh, Privacy Delegate

Signature

Date

19/3/19
Date