



IHACPA

**Independent Health and Aged Care Pricing Authority**

# **Privacy Policy**

Version 5


March 2023

## Contents

<b>Document information</b> .....	<b>2</b>
<b>Glossary</b> .....	<b>3</b>
<b>Introduction</b> .....	<b>5</b>
Purpose .....	5
Privacy framework .....	5
Scope .....	5
Review .....	6
<b>Key Elements</b> .....	<b>7</b>
What is “personal information”? .....	7
Types of information collected by IHACPA.....	7
How IHACPA collects and holds personal information .....	9
How IHACPA may collect and use personal information .....	10
<b>Disclosure of personal information</b> .....	<b>11</b>
<b>Information security</b> .....	<b>12</b>
Privacy Impact Assessments .....	12
Privacy or data breach .....	12
<b>Access and correction</b> .....	<b>13</b>
<b>Privacy complaints</b> .....	<b>13</b>
<b>Roles and responsibilities</b> .....	<b>14</b>
<b>Privacy compliance</b> .....	<b>14</b>

## Document information

### Approval and version history

Version	Effective dates	Change summary	Approvals	Signature	Approval date
1.0	29 August 2012 To 11 March 2014	Alessandra Ryan & Samantha Koevoets	Approved by: Tony Sherbon  Acting Chief Executive Officer		
2.0	12 March 2014 to 11 March 2015	Jane Barry	Approved by:  Tony Sherbon Chief Executive Officer		
3.0	February 2020	Olga Liavas	Approved by:  James Downie Chief Executive Officer	James Downie	25/02/2020
4.0	May 2021	Olga Liavas  Reference to PIA and associated updates	Approved by:  James Downie Chief Executive Officer	James Downie	03/05/2020
5.0	March 2023	Olga Liavas  Changes to policy to reflect amendments to the NHR Act and the Aged Care Act	Approved by:  Prof. Michael Pervan Chief Executive Officer		30/03/2023

### Ownership

Enquiries regarding this document can be made to:

Name: Olga Liavas  
 Position: Executive Officer/Corporate Counsel  
 Email: [olga.liavas@ihacpa.gov.au](mailto:olga.liavas@ihacpa.gov.au)  
 Phone: 02 8215 1129

### Document location

An electronic copy of this document is stored on IHACPA's electronic document records management system (EDRMs) at TRIM D23-4736

## Glossary

**Aged Care Act** means the *Aged Care Act 1997*

**Aged care information** means information relevant to IHACPA's functions under the NHR Act and the Aged Care Act

**APPs** means the 13 Australian Privacy Principles in Schedule 1 to the *Privacy Act 1988*

**APS Privacy Code** means the *Privacy (Australian Public Service – Governance) APP Code 2018*

**Contracted Service Provider** is an entity, or an officer or employee of that entity, that provides services for the purposes (whether direct or indirect) of a contract with IHACPA

**Department** is the Department of Health and Aged Care

**ESF application** is an application for approval to increase extra services fees under section 35-2 of the Aged Care Act

**Hospital data** means Activity Based Funding Data and National Hospital Cost Data Collection data

**IHACPA** is the Independent Health and Aged Care Pricing Authority

**Minister** means the Minister for Health and Aged Care

**NDB** means a Notifiable Data Breach

**NDB scheme** means the scheme in Part IIIC of the Privacy Act that requires IHACPA to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm to any of the individuals

**NHR Act** means the *National Health Reform Act 2011*

**OAIC** means the Office of the Australian Information Commissioner

**Privacy Impact Assessment (PIA)** is a systematic 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

**Personal information** is defined by the Privacy Act to mean information or an opinion about an identified individual, or an individual who is reasonably identifiable

**Pricing and costing data** is information collected for the purposes of advising the Commonwealth in relation to:

- one or more health care pricing or costing matters (whether or not the matters relate to health care services provided by public hospitals)
- one or more aged care pricing or costing matters, including in relation to methods for calculating amounts of subsidies to be paid under the Aged Care Act or the *Aged Care (Transitional Provisions) Act 1997*.

**Privacy Act** means the *Privacy Act 1988*

**Protected Pricing Authority information** is defined by the NHR Act as information that:

- a) was obtained by a person in the person's capacity as an official of the Pricing Authority; and
- b) relates to the affairs of a person other than an official of the Pricing Authority;

but does not include protected information (within the meaning of the Aged Care Act) that is not aged care information.

## Privacy Policy

**RAD application** is an application to charge higher than maximum residential aged care accommodation payments under section 52G-4 of the Aged Care Act

**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

## Introduction

The Independent Health and Aged Care Pricing Authority (IHACPA) is committed to the protection of personal information and complies with the *Privacy Act 1988* (Privacy Act) and the Australian Privacy Principles (APPs).

IHACPA is also committed to ensuring that the statistical hospital data, as well as pricing and costing data and aged care information handled for the purposes of IHACPA's functions under the *National Health Reform Act 2011* (NHR Act), National Health Reform Agreement and the *Aged Care Act 1997* (Aged Care Act) are managed in a manner that is consistent with the APPs, state and territory privacy laws and health data laws. Although these laws may not strictly apply to this data in the form in which it is held by IHACPA, that data is treated with the same care as personal information held by IHACPA.

## Purpose

The purpose of IHACPA's Privacy Policy (the "Policy") is to provide information on:

- what information IHACPA collects
- how IHACPA collects, holds and uses personal information
- how IHACPA handles data breaches that include personal information
- how to lodge a complaint on how IHACPA has handled personal information
- how someone can access or request corrections to their personal information.

## Privacy framework

IHACPA takes all reasonable steps to ensure that it establishes and maintains internal practices, procedures and systems to ensure compliance with the APPs.

IHACPA has developed and implemented a number of supporting policies and procedures to supplement the principles outlined in the Policy, these include;

- Consultant Access to IHACPA Protected Data Rules
- Data Access and Release Policy
- Data Breach Response Plan
- Data Governance Policy
- Information Security Policy
- IT Operations Security Policy
- Privacy Impact Assessment and Guidance
- Privacy Management Plan
- Procedures for handling inquiries, complaints and requests for access and amendment
- Treatment of, and compliance with, the APPs
- Public Interest Disclosure Policy

## Scope

This Policy applies to personal information collected by IHACPA. Where relevant, IHACPA will also apply the Policy to the following data it collects in its role to the extent that it is practicable for IHACPA to do so:

- Activity Based Funding Data and National Hospital Cost Data Collection data (collectively, hospital data)
- hospital pricing and costing information and aged care pricing and costing data (collectively, pricing and costing information).

## Privacy Policy

The requirements under this Policy apply to all IHACPA employees, officers and employees of contracted service providers.

### **Review**

This Policy will be reviewed annually by the Executive Officer/Corporate Counsel but may be reviewed more frequently if required.

## Key Elements

### What is “personal information”?

The Privacy Act defines ‘personal information’ as ‘Information or an opinion about an identified individual, or an individual who is reasonably identifiable’.

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 a number of matters including: the nature and 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).

Where it is technically possible to identify an individual based on the information, but doing so is not practicable, because of: the cost, difficulty, practicality and likelihood of a person or entity doing so, 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 reasonably identifiable.

Personal information relates only to natural persons and in most circumstances it will not apply to deceased persons. However, information about individuals provided in a business or professional capacity is personal information, and will be protected by the APPs.

## Types of information collected by IHACPA

### Personal information

IHACPA only collects personal information where the information is reasonably necessary for, or directly related to, one or more of IHACPA’s functions or activities. Examples include:

- contact details including name, address, phone number, email address, role, organisation or agency, other contact details
- signature
- educational qualifications
- employment history
- procurement records
- consultancy records
- committee membership details
- bank account details
- superannuation details
- creditor and debtor information
- recruitment records
- personnel records

IHACPA may request or receive this personal information from:

- individuals who contact IHACPA with an enquiry
- individuals who act on behalf of a healthcare organisation and register their interest in IHACPA activities
- individuals who deal with IHACPA as part of consultation, including a reference group or as a representative of a stakeholder organisation



## Privacy Policy

- individuals who share data with IHACPA on behalf of a state or territory government department or a healthcare organisation
- researchers who apply for data access and release
- IHACPA's business associates
- members of committees or working groups
- goods and services providers (including contractors)
- current and former employees; and
- applicants for employment.

This information is subject to the Privacy Act and IHACPA has an obligation to ensure that this information is managed in accordance with the Privacy Act.

### **Hospital data**

IHACPA also collects a range of hospital data pursuant to its functions outlined in the NHR Act. The use of hospital data is subject to secrecy provisions contained in the NHR Act which relate to 'protected Pricing Authority information'. The NHR Act recognises the importance of protecting patient confidentiality and imposes strict obligations on the use, disclosure and publishing of information that is likely to enable the identification of a patient (refer to section 279(2) of the NHR Act).

Hospital data contains Activity Based Funding Data and National Hospital Cost Data Collection data including demographic information, clinical information, the nature of care provided and costs.

Importantly, both the patient and the hospital are assigned a unique identifier. This unique identifier is used instead of the patient's name and the name of the hospital. The unique identifiers are not available to the general public. IHACPA has implemented a range of strategies to ensure that data sets are not able to be searched or combined in a way that would allow a person to determine the identity of an individual. For example, hospital data is only used or disclosed in a de-identified fashion.

Where small cell data (that is, data sets with a small number of entries) is present, IHACPA takes measures (such as zeroing or aggregation) to ensure that no identifying data is used or disclosed.

As a result of these measures, the hospital data IHACPA holds is depersonalised and not subject to the Privacy Act. Nevertheless, IHACPA treats its hospital data with care and manages the data consistently with the Privacy Policy, the Privacy Act and the APPs.

### **Pricing and costing information**

With effect from 12 August IHACPA's functions include the providing of advice to the Commonwealth in relation to:

- one or more health care pricing or costing matters (whether or not the matters relate to health care services provided by public hospitals)
- one or more aged care pricing or costing matters, including in relation to methods for calculating amounts of subsidies to be paid under the Aged Care Act or the *Aged Care (Transitional Provisions) Act 1997*.

To perform these functions, IHACPA may conduct, or arrange for the conduct of costing and other studies, consultations and reviews of data.

Specific to its aged care pricing and costing functions under the NHR Act and the Aged Care Act, IHACPA collects:

## Privacy Policy

- Australian National Aged Care Classification Assessment Data
- Aged Care Financial Reporting Data
- Aged Care Funding Instrument Data
- Resource Utilisation and Classification Study Data
- Subsidy, supplement, and service utilisation data.

This data, includes information about Commonwealth funded residential aged care providers and residential aged care recipients. This data may be obtained from a range of sources, including from the Department of Health and Aged Care (the Department), costing studies and individual providers.

Like hospital data, pricing and costing data is 'protected Pricing Authority information' which can only be used and disclosed in accordance with the secrecy provisions in the NHR Act. Pricing and costing data that is aged care information may also be 'protected information' under the Aged Care Act.

Typically, pricing and costing information is obtained in de-identified form. It is also subject to strict controls within IHACPA to prevent potential re-identification. As a result, pricing and costing data is depersonalised and not subject to the Privacy Act. However, like hospital data, IHACPA handles aged care data consistently with this Privacy Policy, the Privacy Act and the APPs.

In certain circumstances such as costing studies where individuals are involved, the individual can request access to information about their hospital stay or aged care service under the FOI Act.

### **How IHACPA collects and holds personal information**

IHACPA collects personal information about individuals directly from those individuals or their authorised representative. IHACPA may also collect personal information if it is required or authorised by or under an Australian law to do so.

When collecting personal information, IHACPA will inform the individual of the purpose for collecting the information, IHACPA's requirements to access the information, how the information will be held, the ramifications if IHACPA fails to collect the information and if the collection of the information is required or authorised by or under Australian law.

IHACPA does not collect sensitive information about an individual unless the individual has consented and the information is reasonably necessary for, or directly related to, one or more of IHACPA's functions.

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

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

## How IHACPA may collect and use personal information

IHACPA may collect and use the personal information in order to:

- assess applications for approval to increase extra services fees under section 35-2 of the Aged Care Act (ESF applications)
- assess applications to charge higher than maximum residential aged care accommodation payments under section 52G-4 of the Aged Care Act (RAD applications)
- perform functions related to providing advice to the Minister in relation to health care pricing or costing matters and aged care pricing matters (see section 131(1A) and section 131A of the NHR Act)
- respond to enquiries and otherwise engage with stakeholders
- communicate information to an individual about any initiative offered by or associated with IHACPA, including invitations to consultation or engagement events
- provide marketing information about goods, services, events or initiatives which may be of interest
- conduct business with its business associates and contractors
- manage requests for data access and release
- manage its employment relationships and responsibilities
- engage and manage its workforce; and/or
- deliver its functions and meet its legal obligations.

For example, the NHR Act authorises IHACPA to establish committees to provide advice or assist in performing its functions. IHACPA collects and uses personal information relating to the committee members in order to establish and maintain current committee member information. Personal information contained in committee files may include contact details and terms of engagement.

If IHACPA is required to pay sitting fees to eligible committee members, IHACPA's file will include member's bank accounts, taxation details and superannuation details in order to pay those sitting fees.

### ESF applications and RAD applications

IHACPA collects, uses and discloses personal information of service provider personnel to assess ESF applications and RAD applications. This includes applications for reconsideration and reviews to the Administrative Appeals Tribunal.

ESF and RAD applications must not include any personal information of care recipients. Applications which contain documents, photographs or other information of care recipients will not be accepted for lodgement.

### Personnel and Contractor files

IHACPA collects and uses personal information to maintain current employee information for business related purposes.

### Stakeholder files

IHACPA collects and uses stakeholder files to maintain current stakeholder information for business related purposes. The personal information relates to contact details and employment details.

### **Personal information in relation to consultation**

Feedback gathered from jurisdictional, stakeholder and public consultations is crucial to the success of IHACPA's work program. IHACPA often collects consultation feedback on a variety of areas in its work program. This can be in the form of written submissions, names, contact details and details of workplaces. All submissions are published on IHACPA's website unless respondents specifically identify any sections they believe should be kept confidential due to commercial or other reasons.

### **Corporate information**

In addition to the above categories, IHACPA collects and uses information about corporate entities. This may contain information relating to a person in their corporate capacity, such as details and job titles for employees of IHACPA's business associates.

While information about individuals comprises personal information, information about corporate entities does not meet the definition of personal information under the Privacy Act. IHACPA treats such information as commercial-in-confidence if it is appropriate to do so.

### **Internet cookies and location information**

A cookie is a very small text file which is stored on an individual's device, when a user first visits a website. Cookies may be used on IHACPA websites, including [www.ihacpa.gov.au](http://www.ihacpa.gov.au). When a visitor returns to a website owned by IHACPA, the cookie enables IHACPA to register that same browser, on which the cookie is stored has returned. Cookies help IHACPA to improve its website and monitor internet traffic.

Visitors to IHACPA's website can block cookies by activating a setting on their browser that allows the visitor to refuse the setting of all or some cookies, however, if the visitor blocks all cookies they may not be able to use the full functionality of IHACPA's websites.

Currently IHACPA's server makes a record of an individual's visit and logs the following information for statistical purposes or systems administration purposes:

- server address
- top level domain name (for example .com, .gov, .au, .uk etc)
- the date and time of the visit to the site
- the pages accessed and documents downloaded
- the previous site visited
- the type of browser being used.

No attempt will be made to identify users or their browsing activities, except in the unlikely event of an investigation where a law enforcement agency may exercise a warrant to inspect the logs.

### **Disclosure of personal information**

Ordinarily, IHACPA discloses personal information to other government agencies or organisations only for the purpose the information was collected.

Personal information may be disclosed for a secondary purpose with the individual's consent, where the individual would reasonably expect that their information will be disclosed, or if disclosure is otherwise required or authorised by or under law.

For example, personal information will be used and/or disclosed:

- to liaise with nominated contacts for ESF applications and RAD applications, including to notify the application outcome.

## Privacy Policy

- to manage new and ongoing employees' employment such as leave applications and approvals and pay related records.
- to monitor employees' phone and internet usage, code of conduct investigations, police checks and security clearances, while undertaking fraud or audit functions or for other purposes relevant to employer powers under the *Public Service Act 1999*.
- to Comcare for worker's compensation matters and/or Comcare rehabilitation providers for rehabilitation purposes and legal advisors for workers' compensation matters.
- to decision makers, which may include external parties, including ministers or the Chair of such committees. Biographical information may be disclosed on IHACPA's website or media announcements regarding particular appointments.
- to other Commonwealth, state or territory government departments and external bodies or contracted service providers responsible for performing the functions, or assisting IHACPA to perform its functions.
- for purposes including IHACPA promotions activities.

IHACPA does not routinely send personal information overseas, but where it does so, it will ensure that it has appropriate procedures and systems in place for ensuring that the information will be handled in accordance with the APPs.

## Information security

IHACPA applies the principles set out in the Australian Government Protective Security Policy Framework and Australian Government Information Security Manual with reference to IHACPA's individual security requirements.

IHACPA will destroy or de-identify personal information if it is no longer required to perform its functions and its retention is not required under Australian law. IHACPA will also ensure that personal information is 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 IHACPA's premises, security firewalls and computer user identifiers and passwords.

IHACPA has adopted a comprehensive Data Governance Policy to ensure that the personal information that it holds is protected. IHACPA's Information Security Policy outlines how IHACPA complies with its information security obligations in respect of the handling and protection of personal information. In addition IHACPA has adopted personnel security procedures to ensure that the information IHACPA holds is protected from misuse.

## Privacy Impact Assessments

IHACPA will also undertake a written Privacy Impact Assessment (PIA) for all 'high risk' projects that involve new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals.

IHACPA keeps a register for the PIAs that it completes on its website ([www.ihacpa.gov.au/privacy-impact-assessment-register](http://www.ihacpa.gov.au/privacy-impact-assessment-register))

## Privacy or data breach

The Notifiable Data Breaches (NDB) scheme in Part IIIC of the Privacy Act requires IHACPA to notify individuals whose personal information is involved in a data breach that is likely to result in 'serious harm' to any of the individuals. Serious harm refers to serious physical, psychological, emotional, financial or reputational harm to an individual or individuals.

IHACPA has implemented a Data Breach Response Plan to manage all data breaches in accordance with the NDB.

If a suspected or known data breach occurs, all employees are required to take action to report suspected data breaches to the Executive Officer and take immediate steps to contain the breach (if applicable). The Executive Officer will immediately notify the Chief Executive Officer (CEO) of the suspected breach and will then undertake an initial assessment based on its seriousness. The CEO will make a decision regarding the response required, including whether notification via the NDB Statement – Form ([www.oaic.gov.au](http://www.oaic.gov.au)) to the Office of the Australian Information Commissioner (OAIC) is necessary.

If serious harm is likely to be caused to an individual or individuals from the data breach, IHACPA will notify the affected individual:

- as far as it is practicable to do so, immediately to advise that a suspected or known data breach has occurred
- the breach includes their personal information, and
- the actions that are being undertaken to limit or mitigate any harm caused by the breach.

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

IHACPA will review the incident to determine possible causes of the breach and revise its internal policies and procedures to prevent reoccurrence. Possible actions will include updating policies and procedures relating to records management and additional staff training on privacy.

## Access and correction

IHACPA will take reasonable steps to ensure that personal information held by IHACPA is accurate, current, complete and relevant.

Individuals who receive marketing materials from IHACPA or are on one or more of IHACPA's distribution lists may opt out or 'unsubscribe' from further communications of this nature.

Individuals can request access to their personal information held by IHACPA, unless an exemption applies (APP 12). They can also request IHACPA to correct their personal information if it is incorrect.

All applications for access and correction should be made in writing and directed to the Privacy Officer (details provided on the following page). IHACPA will generally respond to requests for access or correction in writing within 30 days.

In the event that a person disagrees with the outcome of an access or correction request by IHACPA, they can make a complaint to the OAIC.

Further information is available in IHACPA's Procedures for handling privacy inquiries, complaints and requests for access and amendment.

## Privacy complaints

Individuals can make a complaint about IHACPA's privacy practices to the Privacy Officer. A complaint may be in writing or by phone. Individuals seeking to make a complaint by phone should be invited to make their complaint in writing so that their concerns can be accurately documented and considered.

Once a privacy complaint is received, IHACPA will generally respond within 30 days.

## Privacy Policy

If an individual is dissatisfied with IHACPA's response, they can make a written complaint to the OAIC setting out the details of IHACPA's privacy practices which they think interfere with their privacy. The OAIC will generally expect an individual to complain to IHACPA first, and will likely refer the complaint to IHACPA if this has not occurred.

For more information, see the OAIC website (<https://www.oaic.gov.au/privacy/privacy-complaints>)

## Roles and responsibilities

All IHACPA employees and contractors are responsible for ensuring that IHACPA complies with the Privacy Act by following the requirements of the Privacy Policy.

IHACPA is required under the *Australian Government Agencies Privacy Code* to appoint a Privacy Champion and Privacy Officer. The Privacy Champion provides cultural leadership and promotes the value of personal information. The Privacy Officer is the first point of contact for privacy matters within IHACPA, and is responsible for ensuring day-to-day operational privacy activities are undertaken.

### **Privacy Champion (Executive Director, Costing and Data Infrastructure)**

Name: Julia Hume

Postal Address: PO Box 483 Darlinghurst NSW 1300

Telephone: 02 8215 1159

Email: [julia.hume@ihacpa.gov.au](mailto:julia.hume@ihacpa.gov.au)

### **Privacy Officer (Executive Officer/Corporate Counsel)**

Name: Olga Liavas

Title: Executive Officer/Corporate Counsel

Postal Address: PO Box 483 Darlinghurst NSW 1300

Telephone: 02 8215 1129

Email: [olga.liavas@ihacpa.gov.au](mailto:olga.liavas@ihacpa.gov.au)

## Privacy compliance

IHACPA has established a robust compliance program to ensure that it meets its obligations to manage personal information appropriately and to comply with the APPs. IHACPA reviews how and when it collects personal information to ensure that the collection complies with the APPs.

IHACPA annually reviews its use and disclosure of personal information to ensure that it manages personal information in accordance with the APPs.