Independent Hospital Pricing Authority

Privacy Policy

Version 3.0

February 2020

Contents

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		25/2/2020

Ownership

Enquiries regarding this document can be made to:

Name: James Downie

Position: Chief Executive Officer

Email: james.downie@ihpa.gov.au

Phone: 02 8215 1100

Document location

An electronic copy of this document is stored on IHPA's electronic document records management system (EDRMs) at TRIM D20-1107

Glossary

APPs means the 13 Australian Privacy Principles under the *Privacy Act 1988*

APS Privacy Governance Code means the Privacy (Australian Public Service – Governance) APP code 2018 to be implemented by the OAIC

Contracted Service Provider is an officer or employee of a contracted service provider for a contract with IHPA; and provides services for the purposes (whether direct or indirect) of the contract with IHPA.

IHPA is the Independent Hospital Pricing Authority

NDB means Notifiable Data Breaches

NDB scheme means the *Privacy Amendment (Notifiable Data Breaches) Act 2017* which came into effect on 22 February 2018 and will introduce an obligation for agencies to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm

NHR Act means the *National Health Reform Act 2011*

OAIC means the Office of the Australian Information Commissioner

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

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 of an official of the Pricing Authority; and

b) relates to the affairs of a person other than an official of the Pricing Authority.

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 Hospital Pricing Authority (IHPA) is committed to the protection of personal information and complies with the *Privacy Act 1988* (Privacy Act) and the Australian Privacy Principles (APPs).

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

Purpose

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

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

Privacy framework

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

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

- Data Governance Policy
- Information Security Policy
- IT Operations Security Policy
- Data Access and Release Policy
- Public Interest Disclosure Policy
- Data Breach Response Plan

Scope

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

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

Review

This Policy will be reviewed annually by the Executive Officer 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, where information is provided in a business or professional capacity is also personal information, the APPs will apply.

Types of information collected by IHPA

Personal information

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

- contact details including names, addresses, phone numbers, email addresses, other contact details
- educational qualifications
- employment history
- procurement records
- consultancy records
- committee membership details
- bank account details
- superannuation details
- creditor and debtor information
- recruitment records
- personnel records

IHPA may receive this personal information from:

- individuals who contact IHPA with an enquiry
- individuals who act on behalf of a healthcare organisation and register their interest in IHPA activities
- individuals who deal with IHPA as part of consultation, including a reference group or as a representative of a stakeholder organisation
- IHPA's business associates
- goods and services providers (including contractors)

- current and former employees; and
- applications for employment.

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

Hospital data

IHPA 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. IHPA 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, IHPA 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 IHPA holds is depersonalised and not subject to the Privacy Act. Nevertheless, IHPA treats its hospital data with care and manages the data consistently with the Privacy Policy, the Privacy Act and the APPs.

How IHPA collects and holds personal information

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

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

IHPA 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 IHPA's functions.

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

IHPA 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 Commonwealth Department of Health and meets the security requirements of the Australian Government.

How IHPA may use personal information

IHPA may use the personal information it collects in order to:

- respond to enquiries and otherwise engage with stakeholders
- communicate information to an individual about any initiative offered by or associated with IHPA, 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 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 IHPA to establish committees to provide advice or assist in performing its functions. IHPA 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 IHPA is required to pay sitting fees to eligible committee members, IHPA's file will include member's bank accounts, taxation details and superannuation details in order to pay those sitting fees.

Personnel and Contractor files

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

Stakeholder files

IHPA 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 the IHPA's work program. IHPA often collects consultation feedback on a variety of area's in its Work Program. This can be in the form of written submissions. Names, contact details, details of workplaces are also collected as part of this process. All submissions are published on IHPA'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, IHPA collects and uses corporate information that may contain information relating to a person in their corporate capacity. Examples of such information include contact details and job titles.

Corporate information does not meet the definition of personal information under the Privacy Act. IHPA 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 IHPA websites, including www.ihpa.gov.au. When a visitor returns to a website owned by IHPA, the cookie enables IHPA to register that same

browser, on which the cookie is stored has returned. Cookies help IHPA to improve its website and monitor internet traffic.

Visitors to IHPA'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 IHPA's websites.

Currently IHPA'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

IHPA discloses personal information to other organisations or government agencies only after the individual has been advised, or would reasonably expect, that their information will be disclosed to the receiving entity for the purpose of IHPA undertaking its activities as an employer, or it is otherwise required or authorised by law.

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

- 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 IHPA'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 IHPA to perform its functions.
- for purposes including IHPA promotions activities.

IHPA 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 the security of that information.

Information security

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

IHPA 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. IHPA 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 IHPA's premises, security firewalls and computer user identifiers and passwords.

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

Privacy or data breach

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* established the Notifiable Data Breaches (NDB) scheme in Australia. The NDB scheme requires agencies to notify individuals whose personal information is involved in a data breach that is likely to result in 'serious harm'. Serious harm refers to serious physical, psychological, emotional, financial or reputational harm to an individual or individuals.

IHPA 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) 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, IHPA 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 are being undertaken to limit or mitigate any harm caused by the breach.

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

IHPA 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 to personal information

IHPA will take reasonable steps to ensure that personal information held by IHPA is accurate, current, complete and relevant. Individuals can request access to their personal information held by IHPA. They can also request IHPA to correct their personal information if it is incorrect.

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

To contact IHPA about any privacy inquiry or complaint, or to request access to your personal information, please contact IHPA on +612 8215 1100 or write to PO Box 483, Darlinghurst, NSW, 1300 addressed to the Executive Officer.

Roles and responsibilities

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

IHPA 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 IHPA, and is responsible for ensuring day-to-day operational privacy activities are undertaken.

Privacy Champion (A/Executive Director, Data Analytics)
Name: Julia Hume
Postal Address: PO Box 483 Darlinghurst NSW 1300
Telephone: 02 8215 1159
Email: julia.hume@ihpa.gov.au

Privacy Officer (Executive Officer)
Name: Olga Liavas
Title: Executive Officer
Postal Address: PO Box 483 Darlinghurst NSW 1300
Telephone: 02 8215 1129
Email: olga.liavas@ihpa.gov.au

Privacy compliance

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

IHPA annually reviews its use and disclosure of personal information to ensure that it manages personal information in accordance with the APPs. IHPA's treatment of, and compliance with, the 13 APPs are outlined in Appendix 1.

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

Australian Privacy Principle (APP)	Requirement	Treatment	Compliant?
Consideration of privacy of personal information			
APP1 – Open and transparent management of personal information	Requires IHPA to 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.	IHPA discloses the purposes of collecting personal information. IHPA's Privacy Policy is available on its website and intranet.	Yes
APP2 – Anonymity and pseudonymity	Requires IHPA to provide individuals with the option of not identifying themselves, or of using a pseudonym. Some exceptions apply. These include where IHPA is required or authorised by or under an Australian law to deal with individuals who have identified themselves; or it is impracticable for IHPA 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 a voluntary basis.	Yes
Collection of information			
APP3 – Collection of solicited personal and sensitive information	IHPA must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of IHPA's functions or activities. IHPA must not collect sensitive information about an individual unless the individual has consented to the collection of the information and the information is reasonably necessary for, or directly related to, one or more of IHPA's functions or activities. Under the exceptions listed in APP3.4 IHPA can solicit sensitive information in some cases without complying with APP3.3 where the collection is required or authorised by or under an Australian law. IHPA 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 IHPA is required or	IHPA 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 engagement, payment of reimbursement or sitting fees, appointment of individuals to committees and other similar functions. IHPA requests personal information directly from the individual.	Yes

	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.		
APP4 – Dealing with unsolicited personal information	If IHPA receives personal information that it did not solicit IHPA must determine whether it could have obtained the information under APP3 if IHPA had solicited the information. If IHPA determines that it could not have collected the information and the information is not contained in a Commonwealth record, IHPA must destroy the information or ensure that the information is de-identified but only if it lawful and reasonable to do so.	IHPA appropriately deals with unsolicited personal information including removing unsolicited personal information from IHPA's records management system unless required to retain the information by Australian law.	Yes
APP5 – Notification of the collection of personal information	IHPA must either at or before the collection of personal information notify individuals or a number of matters set out at APP5.2. These matters include the purpose for holding personal information; requirements for access to information and the ramifications of a failure by IHPA to collect the information, if the information is required under Australian law or a tribunal/court order.	IHPA advises the purpose of collecting personal information and ramifications associated with being unable to collect the information.	Yes
Dealing with personal information			
APP6 – Use and disclosure of personal information	IHPA must only use the personal information collected for a purpose other than the primary purpose if the individual has consented to the use or disclosure or if the exceptions apply in APP6.2 or 6.3. These exceptions include whether the individual would reasonably expect IHPA to use the information for the secondary purpose and where disclosure is required under Australian law. In relation to sensitive information if an individual would reasonably expect IHPA to use or disclose the information for a secondary purpose and that purpose is directly related to the primary purpose, that use or disclosure is permitted.	IHPA uses personal information only for the purpose for which it has been collected.	Yes
APP7 – Direct Marketing	Relates to disclosing personal information for the purpose of direct marketing activities.	APP7 applies to private sector organisations only.	Not applicable

APP8 – Cross-border disclosure of personal information	Before IHPA disclose 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.	IHPA undertakes 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	Prohibits an organisation from adopting a government related identifier.	APP9 applies to private sector organisations only.	Not applicable
Integrity of personal information			
APP10 – Quality of personal information	Requires IHPA to take such steps (if any) as are reasonable in the circumstances to ensure person information that is collected, used or disclosed is accurate, current, complete and relevant.	IHPA 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	Requires IHPA to 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. IHPA must also take reasonable steps to destroy or de-identify personal information if it is no longer needed for any purposes for which it may be used or disclosed, it is not contained in a Commonwealth record and IHPA is not required by or under an Australian law to retain it.	IHPA information, regardless of whether it is personal information, is stored in the Electronic Document and Records Management System (EDRMS) provided by Department of Health. IHPA 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	Requires IHPA to give an individual access to personal information upon request of that individual. IHPA can refuse to give access to the information under the *Freedom of Information Act 1982* or any other Commonwealth Act, to the extent that IHPA is required or authorised to refuse access. IHPA must respond to the request for information and give access to the information if it is reasonable and practicable to	IHPA provides an individual access to their personal information upon request. IHPA's Privacy Policy includes contact details for IHPA's Privacy Champion and Privacy Officer in the event an individual wishes to lodge a complaint regarding the	Yes

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