Australian Government

Department of Health

Privacy Policy

Privacy Policy

October 2020

Change history

Date created (version 1)	March 2014
Document owner	Chief Counsel, Legal and Assurance Division
Date of approval (version 2)	November 2017
Current version (version 3)	October 2020

Table of Contents

1. About this Privacy Policy

The Department of Health (**the department, we or us**) is bound by the *Privacy Act 1988* (**the Privacy Act**) and the requirements of the Australian Privacy Principles (**APPs**) in Schedule 1 of the Privacy Act. Under APP 1, we are required to have a Privacy Policy about how we manage *personal information*, as defined in the Privacy Act.

This Privacy Policy provides detailed information about our personal information handling practices, including:

- the kinds of personal information that we collect and hold
- how we collect and hold your personal information
- the purpose for which we collect, hold, use and disclose your personal information
- personal information that may be disclosed to overseas recipients
- how you can contact us if you want to access or correct personal information that we hold about you
- how you can complain about a breach of the Privacy Act and how we will respond to your complaint.

Some activities or functions we administer have their own Privacy Policy, which provides more specific information about our personal information handling practices for that particular activity or function. These include the following:

- Therapeutic Goods Administration
- National Cancer Screening Register
- My Aged Care
- Department of Health Website

This Privacy Policy is only intended to cover how we handle personal information. It is not intended to cover how we handle other types of information.

If you would like to access this Privacy Policy in an alternate format, please contact us using the contact details set out at the end of this document.

2. What we do

Our purpose is to lead and shape Australia's health and aged care systems and sporting outcomes through evidence based policy, well targeted programs and best practice regulation.

We administer a broad range of programs and activities to support Australia's world class health and aged care system which allows universal and affordable access to high quality medical, pharmaceutical, hospital and aged care services while helping people to stay healthy through health promotion and disease prevention activities. Further information about the department can be found on the department's website.

Our diverse set of responsibilities include:

- Aboriginal and Torres Strait Islander health
- access to pharmaceutical services
- access to medical and dental services
- ageing and aged care
- blood and organ policy and funding
- biosecurity and emergency response
- cancer and palliative care
- cancer screening register
- digital health
- health infrastructure, regulation, safety and quality
- health provider compliance
- health protection
- health research
- health workforce capacity
- hearing services policy and funding
- hospitals and acute care
- immunisation
- mental health
- national drug strategy
- population health and sports
- preventive health
- primary health care
- private health
- regulation of therapeutic goods
- sport and recreation.

3. Our obligations under the Privacy Act

This Privacy Policy explains how we comply with the Privacy Act.

The Privacy Act sets out 13 APPs which regulate how we collect, use, disclose and store your personal information, and how you may access and correct personal information we hold about you.

As an Australian Government agency, we are bound by the APPs in the Privacy Act.

We are also bound by the *Privacy (Australian Government Agencies — Governance) APP Code 2017* (**Code**) issued by the Office of the Australian Information Commissioner (**OAIC**) under the Privacy Act. The Code sets out specific requirements and key practical steps that we must take to ensure a best practice approach to privacy governance.

4. What is personal information

We may collect both personal information and sensitive information about you.

Personal information

The Privacy Act defines 'personal information' as:

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

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

For example, the personal information that we collect may include:

- your name, address and contact details (for example, phone, email and fax) to respond to a query about a benefit or program
- information about your personal circumstances (for example, marital status, age, gender and relevant information about your partner and children) in an application for access to a benefit or program
- information about your financial affairs (for example, payment details and bank account details) to determine your eligibility for a benefit or program
- information about your identity (for example, date of birth, police check and security clearance details, country of birth, passport details, visa details and drivers licence) in a recruitment process
- information about your employment (for example, work history, referee comments and remuneration) in a recruitment process or to manage staff
- information about your background (for example, educational qualifications, the languages you speak and your English proficiency) in providing you with support in accessing services or in a recruitment process
- information related to any conflict of interest declarations you make (for example, your financial or other interests, including those of your immediate family members such as spouses/partners or dependants) in the course of employment with the department or to support a committee
- government identifiers (for example, Medicare number and health care identifier) in an application for access to a benefit or program
- information about your entitlements under the legislation we administer.

Depending on the circumstances, information that does not include your name and date of birth may still be considered personal information, if it includes other information about you.

Sensitive information

Sensitive information is a subset of personal information. The Privacy Act defines 'sensitive information' as information or an opinion about a person's:

- racial or ethnic origin
- political opinions or membership of a political association

- religious beliefs or affiliations
- philosophical beliefs
- membership of a professional association or trade association
- union membership
- sexual orientation or practices
- criminal record
- health or genetic information
- biometric information or biometric templates.

For example, the sensitive information that we collect may include:

- your racial or ethnic origin where it is relevant in determining eligibility for a benefit or program or where requested to assist in better targeting access to a benefit or program
- your health (including information about your medical history and any disability or injury you may have, or a family member's medical history) where relevant to assessing an application, making reasonable adjustments in a recruitment process or the management of staff
- membership of a professional association where it is relevant to eligibility for a program or where it is a criterion for eligibility to be engaged in a particular position in the department
- your lesbian, gay, bisexual, transsexual, and/or intersex status where you elect to answer this field in applying for a program or completing a survey
- any criminal record you may have where relevant to assessing your security clearance, or assessing a fit and proper person test relating to a department function or activity.

5. Collection of your personal information

Under the APPs, we will only collect personal information about you where it is reasonably necessary for, or directly related to, a function or activity performed by us. We will only collect sensitive personal information such as health information when you have consented, it is required or authorised by or under law, or where we are otherwise permitted under the Privacy Act.

We take reasonable steps to ensure that personal information we collect about you is accurate, up-to-date, complete, relevant and not misleading.

We collect your personal information only by lawful and fair means. In most cases, we will collect your personal information directly from you. However, there may be circumstances in which we will collect personal information about you from your representative or a third party.

Methods of collection and notification

We collect personal information about you through a range of different channels including:

- paper-based and electronic forms (including online forms)
- face to face meetings
- databases
- telephone, email and facsimile communications
- departmental websites (including online portals)
- social media websites and accounts
- smartphone applications
- data sharing, matching or linkage arrangements with other Australian Government and state and territory government agencies.

The department has a separate Privacy Policy in relation to its handling of personal information collected through its webpages and the operation of cookies.

When the department collects your personal information, where it is reasonable to do so, we will issue you with a privacy notice explaining how we will handle your personal information.

For example, when you commence employment with us, we will issue you with a privacy notice explaining:

- the purpose of us collecting your personal information
- the intended use of your personal information
- to whom your personal information may be disclosed.

Collecting your personal information from third parties

In accordance with the Privacy Act, we will only collect your personal information from a third party where you consent, where required or authorised by or under law or court/tribunal order, or where it is unreasonable or impracticable to collect the information only from you. For example, we may collect personal information about you from a family member with your consent or where we are authorised to collect personal information about you under certain legislation administered by us such as, under the *National Health (Privacy) Rules 2018.* Under the *National Health (Privacy) Rules 2018* we may collect personal information about you from Services Australia for the purpose of clarifying which information relates to you if a doubt arises in the course of linking de-identified information.

In certain circumstances, we may collect personal information about you that is collected by other Australian Government, state and territory government agencies, or other bodies. For example, we may collect information about you in determining eligibility for a benefit or program from:

- Services Australia
- the Department of Veteran Affairs

- the Department of Agriculture, Water and the Environment
- the Department of Home Affairs
- state and territory health departments
- Sport Australia and national sporting organisations
- our portfolio agencies
- health care providers
- health care organisations
- aged care services
- courts and tribunals
- international organisations such as health care facilities and treating practitioners.

This list is not exhaustive and we may collect personal information about you from other bodies.

Collection of unsolicited personal information

We may, on occasion, receive personal information about you from individuals or other entities, without it being requested by us. This information is considered 'unsolicited'. An example of 'unsolicited' personal information is where you write to us seeking further information on the services we provide or to provide feedback on your experience with the department and you provide information that is not required to respond to your query or feedback.

We will deal with unsolicited personal information in accordance with the APPs. We will destroy your personal information unless it is contained in a Commonwealth record under the *Archives Act 1983* or unless we consider that we could have lawfully collected it under the APPs.

Collection of personal information about children, young and vulnerable people

We may collect personal information about children and young people. For example, the department collects personal information related to notifiable diseases and adverse events from the use of therapeutic goods regardless of age, for the purposes of managing public health risks.

We will only collect personal information about children when required or authorised by or under law, or otherwise in accordance with the Privacy Act.

If an individual lacks capacity to consent for any reason, our policy is to seek consent from an authorised person, for example a legal guardian or a carer.

Collection of de-identified personal information

We may also collect information that has been de-identified and reported to us by organisations coordinating or providing health services funded by the department, to be used for statistical and evaluation purposes.

Purposes for which personal information may be collected by the department

We may collect personal information about you for the following purposes:

- employment, work health and safety and personnel matters
- the performance of our legislative and administrative functions and activities
- administration of goods regulation and the National Notifiable Disease Surveillance System
- policy development, research, and evaluation of our programs and services
- the management of contracts, funding agreements and procurement processes
- a range of statutory and non-statutory committees, boards, reference and working groups
- individuals signed up to distribution and mailing lists
- the management of fraud and compliance investigations and audits
- correspondence from members of the public to us and our Ministers, or correspondence otherwise referred to us by other departments or Ministers
- complaints (including privacy complaints) made and feedback provided to us
- requests for access to documents held by us including requests under the *Freedom of Information Act 1982*
- the provision of legal advice by internal and external lawyers.

6. Remaining anonymous or using a pseudonym

You may wish to remain anonymous or use a pseudonym when you interact with us. When we deal with you anonymously, we do not collect any personal information or identifiers from you. Using a pseudonym means to use a different name or term instead of your actual name.

Where possible, we will allow you to interact with us anonymously or using a pseudonym. For example, we may not need your personal information when you:

- provide a tip-off about an alleged fraud, misconduct or contravention of legislation administered by us,
- seek general information about a program, policy or consultation process, or
- participate in a public consultation process.

However, in some circumstances, it may be impracticable to remain anonymous or use a pseudonym, or we may be legally required to deal with you in an identified form.

For example, we may not be able to give you access to your personal information under the *Freedom of Information Act 1982* unless we are satisfied that the requested information relates to you. It may also be necessary to collect some personal information from you in order to resolve a complaint that you have made. We will notify you at the time of collection if this is the case.

7. Use and disclosure of your personal information

The purpose for which we collect your personal information is important as it restricts how we can use and disclose your personal information. Unless an exception applies in the Privacy Act, we will:

- only use or disclose your personal information for the purpose for which it was collected, and
- where reasonable to do so, notify you of this purpose at the time of collection, or as soon as practicable after collection.

We will only use or disclose your personal information for another purpose where we are able to do so in accordance with the Privacy Act. As a general guide, we routinely disclose personal information to the same bodies from which we may collect personal information about you, as listed in Part 5 of this Privacy Policy. We may also disclose your personal information to:

- the Australian Bureau of Statistics
- the Australian Institute of Health and Welfare
- contracted service providers that provide services on behalf of the department in relation to our programs
- contracted service providers that assist in the department's human resources, communications, information technology, legal or other corporate functions
- review, audit, investigation and intelligence agencies and bodies
- Royal Commissions

This list is not exhaustive and we may disclose your personal information to other Australian Government agencies or to other bodies in accordance with the Privacy Act.

8. Purposes for which the department may collect, use or disclose your personal information

There are a number of purposes for which we may collect, use and disclose your personal information, which we describe below. References to use and disclosure of your personal information include references to our employees' and contractors' handling of your personal information. We will only collect, use or disclose your personal information in accordance with the Privacy Act and other legislation we administer.

Recruitment processes and on-boarding

Personal information collected about applicants during the recruitment process may be used and disclosed by the department as part of both the recruitment and the on-boarding process.

For example, personal information collected during the recruitment process may be disclosed to other Australian Government agencies through the creation, use and sharing of a merit list as well as with recruitment agencies engaged by the department to assist with the recruitment process.

Employment, work health and safety and personnel functions

Personal information may be used and disclosed to manage new and ongoing employees' employment such as leave applications and approvals as well as payroll and pay related records.

Personal information may also be used and disclosed for work health and safety purposes, 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.

For example, for workers' compensation matters, personal information may be disclosed to Comcare, rehabilitation providers and legal advisors.

Managing the operation of departmental or portfolio committees, boards, reference and working groups

Personal information may be used and disclosed to manage the operation of departmental or portfolio committees, boards, reference and working groups.

Personal information may be used and disclosed to decision makers within the committees, boards and groups. These may include external parties, including Ministers or the chair of such committees.

For example, information about members of a committee may be used and disclosed by officers in the department to arrange accommodation and flights for an upcoming meeting.

Undertaking legislative, administrative, policy and program related functions, duties and powers

Personal information may be used and disclosed in the course of undertaking legislative, administrative, policy and program related functions, duties and powers.

Personal information may be disclosed to other Australian Government, state or territory government agencies and external bodies or contracted service providers responsible for performing the relevant functions, or assisting the department to perform the relevant functions.

For example, personal information may be used and disclosed in administering the Medicare Benefits Schedule, the Pharmaceutical Benefits Scheme, My Aged Care or other health related programs that comprise the department's functions.

Undertaking fraud and compliance investigations both internally and externally

Personal information may be used and disclosed in the course of undertaking fraud and compliance investigations into employees, consultants, health providers as well as contractors and other bodies. Personal information may be disclosed to other Australian Government, state and territory government agencies, enforcement bodies, review, audit, investigation and intelligence bodies or consultants as well as the Commonwealth's legal advisers for these purposes.

For example, Medicare claims information may be used in undertaking compliance activities to identify and seek repayment of benefits claimed incorrectly by health professionals under the Medicare Benefits Schedule.

Undertaking health promotion activities and campaigns

Personal information may be used and disclosed for purposes including health promotion activities. For example, where you consent, personal information may be used and disclosed in undertaking campaigns targeting Aboriginal and Torres Strait Islander health and mental health.

Approach to market/Contract management

Personal information may be used as a result of an approach to market process, even where the applicant is not successful. Personal information may also be used to monitor compliance with clauses in a contract.

Managing and responding to correspondence and enquiries from members of the public

Personal information may be used and disclosed for the purpose of corresponding with the public and distributing departmental publications.

For example, where appropriate, personal information may be used and disclosed in accordance with the Freedom of Information Act 1982 (FOI Act) in the course of a freedom of information request or in responding to a complaint about a program.

To undertake policy development, program evaluation, research, surveys (including one off and longitudinal) and reports of health activities and businesses

Personal information may be used in the course of undertaking policy development, program evaluation, research, surveys (including one off and longitudinal) and reports of health activities and businesses.

For example, personal information may be disclosed to individual researchers or other Australian Government, state and territory government agencies for the same purposes. Our Data Access and Release Policy provides more detailed information about the matters we consider when assessing requests by researchers for health program and health performance data.

Compiling statistics and evaluation of the provision and commissioning of health care services

Personal information may be used and disclosed by the department for the purpose of compiling statistics and evaluation of the provision and commissioning of health care services. Personal information may be disclosed to Australian Government, state or territory government agencies and external bodies or contracted service providers responsible for performing the relevant functions, or assisting the department to perform the relevant functions. For example, the department may issue a public interest certificate to researchers under the National Health Act 1953 or the Health

Insurance Act 1973 to provide them with personal information about you for the purpose of undertaking research about public health matters.

We will only disclose information for research purposes in accordance with the Privacy Act and other relevant legislation we administer. Recipients of personal information disclosed under a public interest certificate are subject to strict requirements in relation to how the information will be used and are generally prohibited from further disclosing the information to any other parties.

Where authorised or required by or under an Australian law or a court/tribunal order

Personal information may be used and disclosed where this is authorised or required by or under an Australian law. These third parties may include contracted service providers, Australian Government agencies and state and territory agencies as well as researchers.

For example, we may disclose personal information to state and territory disciplinary bodies for the purposes of investigations into professional misconduct by health professionals, in accordance with the *Health Insurance Act 1973*.

9. Data linkage and integration

We may on occasion create new datasets by linking data from different sources including data lawfully collected by us from other Australian Government, state and territory government agencies.

Data linking may involve de-identified information or your personal information. We will only engage in data linking in accordance with the Privacy Act and other legislation we administer and for purposes including:

- informing policy development
- statistical and research purposes
- implementing and evaluating the effectiveness of our programs and services
- compliance purposes.

We engage in data linking projects with other Australian Government, state and territory government agencies, researchers and other external parties where our participation is in accordance with the Privacy Act and other relevant legislation. Such projects are often called 'data integration projects' and are usually undertaken by us for policy analysis, statistical and research purposes and may involve linking of personal information or de-identified information. Data integration projects in which we are a partner agency include the Multi-Agency Data Integration Project (**MADIP**) and the National Integrated Health Services Information Analysis Asset.

We may also undertake data matching activities with other agencies to ensure the integrity of claiming by health providers under Medicare programs, including the Pharmaceutical Benefits Scheme and other health payment programs. Such activities are undertaken in accordance with the Privacy Act or other relevant legislation and involve comparing data held by the department with data sourced from other agencies including:

- the Therapeutic Goods Administration
- the Department of Home Affairs
- the Australian Health Practitioner Regulation Agency
- the Department of Veterans' Affairs.

10. Disclosure of your personal information overseas

We disclose personal information to overseas recipients in limited circumstances. These may include when you give consent, where your personal information is not identifiable, or where disclosure is required or authorised by or under law.

If we are unable to obtain your consent or if it is impractical to do so, we will only provide your personal information to an overseas recipient in accordance with the *Privacy Act*.

Situations in which we may disclose personal information overseas include:

disclosures to foreign governments, law enforcement agencies, or international bodies when required or authorised by or under law, or pursuant to international agreements relating to information sharing:

- disclosures that are required as a result of services provided by us through overseas programs such as the Medical Treatment Overseas program, or where relevant to our role relating to human biosecurity
- disclosures that are required to foreign governments and international bodies such as the World Health Organisation, in relation to notifiable diseases (in order to manage public health risks), as well as certain information related to therapeutic goods
- disclosures to foreign governments for the purposes of overseas travel arrangements for staff.

For example, we may disclose your personal information under the *National Health Security Act 2007* to a foreign government to manage risks to public health associated with communicable diseases. Any such disclosures are made in accordance with Australia's international obligations in relation to notifiable diseases.

As part of the Medical Treatment Overseas Program, once your application is approved by us we will issue a letter with personal information about you to the relevant treating facility in the overseas country to allow you to receive the relevant treatment. Countries in which applicants may seek treatment and to which we may disclose personal information include the United States of America.

11. Storage of your personal information

Personal information collected and held by third parties

Personal information may be held by us or by people or organisations acting on our behalf, for example, contracted service providers.

Under the Privacy Act, we are required to take measures to ensure that when your personal information is held by a third party, that the third party complies with the same privacy requirements applicable to the department.

We include privacy clauses in our contractual agreements with third parties, including funding agreements, consultancy and services contracts and various other ad-hoc contractual agreements. This is to ensure that the third parties handle personal information in accordance with relevant privacy obligations.

Storage, retention and destruction of personal information

Personal information held by the department is stored on electronic media, including the department's Electronic Document and Records Management System, Enterprise Data Warehouse, business applications and cloud computing solutions. Personal information is also held on paper files.

We store and dispose of your personal information in accordance with the *Archives Act 1983* and relevant records authorities. For more information, see the National Archives of Australia website.

We will take reasonable steps to destroy or de-identify your personal information if we no longer need it for the purpose for which it was collected, unless required or authorised by or under law or a court/tribunal order to retain the information, or if it is contained in a Commonwealth record. When personal information is no longer required to be retained as part of a Commonwealth record, it is destroyed in accordance with the *Archives Act 1983*.

Data security

Electronic and paper records are protected in accordance with Australian Government security policies, including the *Attorney-General Department's Protective Security Policy Framework and the Australian Signals Directorate's Information Security Manual*.

The department has a layered in depth security approach to protecting information from misuse, interference and loss from unauthorised access, modification or disclosure.

Certain personal information is held on behalf of the department by our contracted Information, Communications and Technology service providers, who are contractually required to protect the information to the same standards as the department in accordance with the APPs.

We have controls in place for accessing information appropriate to the type and sensitivity of the information. Access to personal records by staff and contractors is restricted to officers on a 'need to know' basis. We also protect your personal information through steps that include password protection for electronic files, securing paper files in locked cabinets and other access restrictions.

12. Access and correction

You have a right under the FOI Act and the Privacy Act to access personal information that we hold about you. You also have a right to request correction of your personal information if it is inaccurate, out of date, incomplete, irrelevant or misleading.

You can request access to documents containing your own personal information by emailing our FOI Unit at foi@health.gov.au. There is no charge under the FOI Act for making a request or for the provision of your own personal information. Your right of access under the FOI Act is subject to our right to refuse access under the FOI Act. More information about making FOI requests is available on our FOI web page on the department's website or by telephoning (02) 6289 1666.

Alternatively, you can request access to your personal information under the Privacy Act by contacting the department using the contact details set out at the end of this Privacy Policy. We will take reasonable steps to provide you with access and/or make a correction to your personal information within 30 calendar days, unless we consider there is a sound reason under the *Privacy Act* or other relevant law to withhold the information, or not make the changes.

For example, we may refuse access to your personal information where the record includes another individual's personal information or where refusal is required or authorised by the FOI Act or any other law.

If we do not provide you with access to your personal information, or refuse to correct your personal information, where reasonable we will:

- provide you with a written notice including the reasons for the refusal
- provide you with information regarding available complaint mechanisms
- at your request, take reasonable steps to associate a statement with the personal information that you believe to be inaccurate, out of date, incomplete, irrelevant or misleading.

If we correct your personal information, at your request, we will also take reasonable steps to notify other agencies or organisations that we have previously disclosed your personal information to, and that are bound by the Privacy Act, of the correction.

Updating your personal information

It is important to tell us if your 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.

13. Personal information may be protected by other legislation

Secrecy provisions

Personal information collected by us may be protected by secrecy provisions under legislation that we administer. Secrecy provisions further restrict how we handle your

personal information. These obligations apply alongside the Privacy Act. A full list of the department's portfolio legislation can be found in the Administrative Arrangements Order available on the Federal Register of Legislation.

National Health (Privacy) Rules 2018

The *National Health (Privacy) Rules 2018* **(the Rules)** issued by the OAIC under section 135AA of the *National Health Act 1953* regulate how we handle certain information obtained under the Medicare Benefits Program and the Pharmaceutical Benefits Program. Where relevant, we will handle your personal information in accordance with the Rules.

14. The Notifiable Data Breaches Scheme

The Notifiable Data Breach Scheme (the **NDB Scheme**) in Part IIIC of the Privacy Act commenced on 22 February 2018. In accordance with the NDB Scheme, we investigate and undertake assessments of suspected and actual data breaches, and notify 'eligible data breaches' to the OAIC and affected individuals.

We take seriously and deal promptly with any unauthorised access to, disclosure of, or loss of personal information (**data breach**). Examples of data breaches include a document containing personal information being sent to the wrong recipient due to human error, or a failure to remove or redact personal information from a record before disclosing it.

We also have additional notification obligations to report data breaches to the OAIC under the *National Cancer Screening Register Act 2016*.

15. Privacy Impact Assessments

A Privacy Impact Assessment (**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.

In accordance with the Code, we undertake a PIA for all projects where there is a new or changed way of handling personal information that is likely to have a significant impact on the privacy of individuals.

We maintain a register of PIAs, which lists PIAs completed by us in relation to any higher privacy risk projects since the Code came into effect on 1 July 2018. Where appropriate, we will make the PIA publically available. For example, the department conducted and published a PIA for the COVIDSafe Application.

16. Complaints

How you can complain about the treatment of your personal information

If you believe that we have breached the Privacy Act, the Code or otherwise mishandled your personal information, you can contact us using the contact details set out below.

Each complaint will be dealt with on a case-by-case basis. All complaints will be investigated by us and you will be advised of the outcome.

All privacy complaints are taken seriously. You should not be victimised or suffer negative treatment if you make a complaint.

Making a privacy complaint

If you believe that we have breached the APPs or mishandled your personal information, you should take the following steps:

1. Contact us: in the first instance, any privacy concern or complaint should be reported directly to the department. This can be done using the contact details set out at the end of this document.
2. Submit your concern or complaint in writing: in order to be able to fully investigate your complaint, we would prefer that you make your complaint in writing using the contact details set out at the end of this document. The complaint should include information about the claimed privacy breach and your contact details. Please note that if you do not provide sufficient information or if you submit an anonymous complaint, we may not be able to fully investigate and respond to your complaint.
3. Reasonable amount of time: we will acknowledge your concern or complaint upon receipt. This may involve email or telephone correspondence with you. We will also provide you with updates as to our investigation into your privacy complaint, if you provide your contact details. We will try to respond to your privacy concern or complaint as soon as practicable.

We will use the information from your complaint to investigate and seek to resolve the issues you have raised. This may include speaking to relevant areas of the department and considering their processes as well as speaking to third parties where relevant.

We will use the information you provide in your complaint to provide feedback to staff or our business areas. If you are not satisfied with our response, you can complain directly to the OAIC. The OAIC's details are:

Means of contact	*Contact details*
Telephone:	1300 363 992
Email:	enquiries@oaic.gov.au
Post:	Australian Information Commissioner GPO Box 5218 Office of the Australian Information Commissioner Sydney NSW 2001

Please note that the OAIC generally requires that a complaint first be raised with us before the OAIC will investigate.

How to contact us

You can contact us on:

Phone:	(02) 6289 1555 or freecall 1800 020 103
Online:	See the online enquiries form on the department's website.
Email:	privacy@health.gov.au
Post:	Privacy Officer Department of Health GPO Box 9848 CANBERRA ACT 2601