



Privacy Policy



Document details

Document owner: Chief Counsel, Legal Division

Change history:

Version	Date of approval
Document created (version 1)	March 2014
Document updated (version 2)	November 2017
Document updated (version 3)	October 2020
Document updated (version 4)	October 2025

Contents

Document details.....	ii
Contents.....	iii
1. About this Privacy Policy	1
2. What we do	1
3. Our obligations under the Privacy Act.....	2
4. What is personal information	2
5. Collection of your personal information.....	5
6. Remaining anonymous or using a pseudonym	9
7. Use and disclosure of your personal information	9
8. Purposes for which the department may collect, use or disclose your personal information	10
9. Data linkage and integration	14
10. Disclosure of your personal information overseas	15
11. Storage of your personal information	16
12. Artificial intelligence and emerging technology	17
13. Access and correction	17
14. Personal information may be protected by other legislation	18
15. The Notifiable Data Breaches Scheme	18
16. Privacy Impact Assessments	19
17. Complaints	19
18. How to contact us	20

1. About this Privacy Policy

The Department of Health, Disability and Ageing (**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, Disability and Ageing Website](#)
- [Australian Immunisation Register](#)

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. Insert the introduction here.

2. What we do

Our purpose is to lead and shape Australia's health, disability and aged care systems 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, disability and aged care system which allows universal and affordable access to high quality medical, pharmaceutical, hospital, aged care, disability and carer 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
- biosecurity and emergency response
- blood and organ policy and funding
- cancer and palliative care
- cancer screening register
- carers
- 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
- people with disability
- population health
- preventive health
- primary health care
- private health
- regulation of therapeutic goods

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 and the *Privacy (Australian Government Agencies — Governance) APP Code 2017 (Code)*.

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 or a request for information
- 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
- your image, voice, or use of sign language when you participate in meetings, workshops or interviews with the department where these are recorded,
- information about your financial affairs (for example, payment details and bank account details) to determine your eligibility for a benefit or program
- your name, job title or organisation, accessibility requirements and contact details when you join a mailing list, give feedback in a consultation process or participate in stakeholder meetings
- information about your identity (for example, date of birth, gender, police check and security clearance details, country of birth, passport details, visa details and drivers’ licence) for the purpose of:
 - a recruitment process; or
 - to provide you access to government systems in order to deal with the department; or
 - to provide human resources and corporate services (for example, corporate credit cards and travel bookings), in the course of your employment with the department or a portfolio agency which the department provides these services to under a shared services agreement,
- information about your employment (for example, work history, referee comments and remuneration) and banking information in a recruitment process, committee appointments 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, in a recruitment process or committee appointments
- information about your caring responsibilities in providing you with support in accessing services or when you respond to a consultation 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). Information about conflicts of interest may be collected:
 - in the course of employment with the department, or
 - in relation to your appointment to a committee, or
 - to avoid conflicts of interest impacting decisions (for example, decisions about public health policies including in relation to tobacco control).
- information or allegations about an individual's activities to investigate suspected wrongdoing under the *Public Interest Disclosure Act 2013*.

- government identifiers (for example, Medicare number, aged care client identifier, Multi-Purpose Services (**MPS**) Program client identifier and health care identifier) in an application for access to a benefit or program.
- identity and health information, including body samples (tissue, blood and body fluid samples), as part of screening travellers who are suspected of having a listed human disease under the *Biosecurity Act 2015*.
- 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.

In some circumstances we may collect and store personal information for other portfolio agencies where the department has an agreement to provide services to these agencies. One example of this is the department will facilitate the Aged Care Quality and Safety Commission's collection and storage of information about aged care workers screening via the Government Provider Management System (**GPMS**).

SENSITIVE INFORMATION

Sensitive information is a subset of personal information. The Privacy Act defines 'sensitive information' as information or an opinion about an individual'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 information (including information about health services needed or provided) 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 medical certificates, information about your medical history, any illness, disability or injury you may have, a family member's medical history or your disability support or aged care needs) where relevant to:
 - assessing an application,
 - determining eligibility for services,
 - making reasonable adjustments in a recruitment process,
 - accommodating accessibility requirements when you interact with the department,
 - managing staff,

- public interest disclosures submitted to or investigated by the department or
- as part of a consultation process (such as consultations about lived experience of certain health conditions or consultations about medicines being considered by the Pharmaceutical Benefits Advisory Committee (**PBAC**) for inclusion on the Pharmaceutical Benefits Scheme (**PBS**))
- the National Notifiable Diseases Surveillance System
- 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 gender identity, sexual orientation or intersex status where:
 - you elect to answer this field in applying for a program or completing a survey or consultation process
- 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 will only collect the minimum amount of personal information necessary.

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 and virtual meetings and associated meeting minutes and recordings
- databases
- security systems used to ensure security of the department's information and premises
- telephone, email and facsimile communications
- departmental websites (including online portals)
- social media websites and accounts
- applications, including smartphone applications
- third party platforms used to conduct consultations

- data sharing, matching or linkage arrangements with other Australian Government and state and territory government agencies.

The department has a separate [Website 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 *Australian Immunisation Register Act 2015*. Under this Act the department is authorised to collect personal information for the purposes of the Australian Immunisation Register.

Examples of when we may collect personal information from third parties where it is unreasonable or impracticable to collect it directly from you include collecting online or open-source intelligence for compliance activities or investigations, or to identify experts to peer-review Communicable Diseases Intelligence (**CDI**) journal articles.

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 from other agencies to determine eligibility for a benefit or program. The agencies or bodies we may collect information from include:

- Services Australia
- the Department of Social Services
- the Department of Veterans' Affairs
- the Department of Agriculture, Fisheries and Forestry
- the Department of Home Affairs
- the National Indigenous Australians Agency
- state and territory health departments
- our portfolio agencies (for example the Independent Hospital Pricing Authority, the Aged Care Safety and Quality Commission, the National Disability Insurance Agency (**NDIA**), the National Disability Insurance Scheme (**NDIS**) Quality and Safeguards Commission, the Australian Institute of Health and Welfare),

- health, aged care or disability providers
- health, aged care or disability organisations
- courts and tribunals
- law enforcement agencies
- Ministers
- universities
- legal guardians or carers
- domestic and 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

If we receive personal information that we did not ask to receive we will deal with this unsolicited personal information in accordance with the APPs. An example of 'unsolicited' personal information is where you contact us to ask a question about our programs or to provide feedback and you provide personal information that is not required to respond to your query or feedback.

COLLECTION OF PERSONAL INFORMATION ABOUT CHILDREN, YOUNG AND VULNERABLE PEOPLE

We may collect personal information about children, young and vulnerable people in order to deliver or inform improvements to services or programs.

Vulnerable people whose information we may collect include older people, those with health conditions or disabilities, people of culturally and linguistically diverse backgrounds, First Nations people or people facing social or financial hardship.

Examples of where the department collects personal information about children, young or vulnerable people include:

- we collect 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 collect personal information about children born alive as a result of a mitochondrial donation technique for the purposes of the Mitochondrial Donation Donor Register;
- we collect personal information about people with disability to deliver or inform improvements to disability services;
- we collect personal information about older people to deliver or inform improvements to aged care services.

We will only collect personal information about children, young and vulnerable people with consent, or 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 collect information that has been de-identified and reported to us by organisations coordinating or providing health, disability, aged care or other services funded by the department, to be used for statistical, policy development 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, security and personnel matters
- providing human resources and corporate services for employees of the department, and of other portfolio agencies where the department has an agreement to provide these services to those agencies
- the performance of our legislative and administrative functions and activities,
- the administration and delivery of programs, including to check eligibility for programs
- implementing changes to programs, policies or legislation
- monitoring and reporting on mental health and suicide prevention systems
- administration of the National Notifiable Diseases Surveillance System
- the regulation of therapeutic goods
- policy development, research, consultation 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, including healthcare provider compliance functions
- 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* ('FOI Act')
- the provision of legal advice by internal and external legal advisors.

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 legal or chosen 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
- provide feedback on a policy or program, 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. We may need to collect some personal information or identifiers from you in order to deliver a particular program. 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
- the Department of Prime Minister & Cabinet in relation to committee appointments

- portfolio bodies (such as the Independent Health and Aged Care Pricing Authority, the Aged Care Quality and Safety Commission, the NDIA),
- contracted service providers that provide services on behalf of the department in relation to our programs
- contracted service providers, including financial institutions, that assist in the department's human resources, communications, information technology, legal, travel or other corporate functions
- review, audit, investigation and intelligence agencies and bodies
- researchers
- state and territory governments
- 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

We collect, use and disclose your personal information for a range of purposes described 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,
- to conduct code of conduct investigations,
- to obtain police checks,
- to conduct suitability assessments before and during employment,
- for international working arrangements,
- for security purposes including detecting and responding to security threats and managing security clearances,
- while undertaking fraud or audit functions,
- for other purposes relevant to employer powers under the *Public Service Act 1999*, or
- to seek legal advice in relation to any of the above matters.

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

MANAGEMENT OF HUMAN RESOURCES AND CORPORATE SERVICES FOR EMPLOYEES OF THE DEPARTMENT AND OTHER PORTFOLIO AGENCIES

Personal information may be used and disclosed to provide human resources and corporate services for employees of the department and of portfolio agencies where the department has an agreement to provide these services to those agencies, in the course of their employment.

For example, personal information of employees may be disclosed to contracted service providers, such as financial institutions, to organise work related travel.

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 or to seek legal advice in relation to appointments.

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. This includes for the purposes of checking eligibility for, and delivering, programs, services and supports.

If you were receiving aged care services prior to 1 November 2025, we will also use and disclose your personal information to transition you to services under the new *Aged Care Act 2024*.

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, the Australian Immunisation Register, My Aged Care or other programs that comprise the department's functions.

UNDERTAKING FRAUD AND COMPLIANCE ACTIVITIES 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 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 FOI Act in the course of a freedom of information request or in responding to a complaint about a program.

TO UNDERTAKE POLICY DEVELOPMENT, SERVICE DELIVERY, PROGRAM EVALUATION, RESEARCH, SURVEYS (INCLUDING ONE OFF AND LONGITUDINAL) AND REPORTING

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.

Personal information may also be disclosed to Australian Government, state and territory government agencies, research institutes, other entities and individual researchers for the same purposes. Our Data Governance Framework sets out the standards and expectations for effective management of data in the department, including the embedding of safe practices for use, re-use and sharing of data.

COMPILING STATISTICS, ENABLING RESEARCH AND EVALUATION OF THE PROVISION AND COMMISSIONING OF HEALTH, DISABILITY AND AGED 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, disability and aged 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*.

In accordance with the *Data Availability and Transparency Act 2022*, we may disclose information to accredited users for three permitted purposes – delivering government services, informing government policies and programs, and undertaking research and development. Personal information is only shared in accordance with the privacy protections under that Act.

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. Examples of key Australian Government data integration projects supported by the department are the Person Level Integrated Data Asset, the National Health Data Hub and the National Disability Data 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. Our ['Data matching notice'](#) explains how we data match for Medicare compliance purposes. Our [Data matching public register](#) records data matching undertaken for Medicare compliance purposes. 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:

- Department of Home Affairs
- Australian Health Practitioner Regulation Agency
- Department of Social Services
- Services Australia
- Australian Digital Health Agency
- NDIA
- 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
- disclosure to staff of Food Standards Australia New Zealand who are located in New Zealand
- 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 and working arrangements for staff
- publication on the internet of submissions provided during consultations or details of authors of published reports or articles
- disclosures to expert reviewers or assessors located overseas for the purpose of assessing research applications
- where third party providers store personal information on servers located overseas (e.g. where you subscribe to receive publications and news managed by a third-party provider and you consent to your personal information being used for these purposes, including being stored in servers located overseas).

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.

We take contractual measures to ensure that when your personal information is held by contracted service providers and grant recipients, that these parties comply with the same privacy requirements applicable to the department.

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, Data Warehouses, business applications and cloud computing solutions. Personal information is also held on paper files. The department's storage of personal information complies with the Protective Policy Security Framework.

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 Department of Home Affairs' 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 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. Artificial intelligence and emerging technology

The [department's Artificial Intelligence \(AI\) transparency statement](#) explains how we will adopt and use AI in line with the Australian public's and Government's expectations. Any use of AI to support the department undertaking its functions and activities, including where this involves the use of personal information, will be done in accordance with our transparency statement. This will be updated as we continue to develop policies on AI usage and implement AI technology.

13. 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.

Find out how to make an [FOI request here](#).

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.

So we can process a request to access or correct personal information, we will need to collect information to verify your identity.

If you are requesting access or correction on behalf of someone else, we will need to collect a copy of the relevant authorisation for you to act on their behalf, such as a Power of Attorney.

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 not provide 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.

14. Personal information may be protected by other legislation

SECURITY 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 2025

The *National Health (Privacy) Rules 2025* (**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.

15. The Notifiable Data Breaches Scheme

We take seriously and deal promptly with any unauthorised access to, disclosure of, or loss of personal information (**data breach**). In accordance with the Notifiable Data Breach Scheme (**the NDB Scheme**) in the Privacy Act, we investigate and undertake assessments of suspected and actual data breaches and notify 'eligible data breaches' to the OAIC and affected individuals.

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

16. 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.

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. These are listed on our [register of PIAs](#). Where appropriate, we will make the PIA publicly available.

17. Complaints

HOW TO MAKE A PRIVACY COMPLAINT

If you want to make a complaint about how we have handled your personal information, you should contact us in writing using the contact details set out at the end of this document.

Please provide information about the claimed privacy breach and your contact details. 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.

We will acknowledge your complaint quickly, and work with you to resolve your complaint. We will keep you updated on the progress of your complaint.

We may need to speak to relevant areas of the department and third parties where relevant to investigate and resolve your complaint.

We may also use the information you provide in your complaint to provide feedback to staff or our business areas.

If you are not happy with our response to your complaint, you may make a complaint to the Office of the Australian Information Commissioner (OAIC) by calling 1300 363 992 or visiting the [OAIC website](#).

Usually, the OAIC requires you to try to resolve your complaint with us first before they will investigate.

18. How to contact us

You can contact us on:

Our contact details:

Method	Contact details
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, Disability and Ageing GPO Box 9848 CANBERRA ACT 2601

Health.gov.au

All information in this publication is correct as at October 2025

