Australian Government
Department of Health, Disability and Ageing

Inquiry into client privacy in the Australian public sector

Submission from the Department of Health, Disability and Ageing
to the Joint Committee of Public Accounts and Audit

14 MAY 2026

Australian Government
Department of Health, Disability and Ageing

Contents

Australian Government
Department of Health, Disability and Ageing

Introduction

The Department of Health, Disability and Ageing (**department**) administers a broad range of programs and activities to support Australia's world class health, disability and aged care system. This system provides 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.

The delivery of the department's functions is underpinned by a strong culture of privacy awareness and a framework of both statutory and policy controls to ensure the protection of personal information. The department's approach to managing privacy risks is integral to the preservation of public trust in the Commonwealth as a custodian of the personal information of Australians.

The department welcomes the opportunity to make a submission to the Joint Committee of Public Accounts and Audit's *Inquiry into the management of client privacy in the Australian public sector.* This submission outlines how the department complies with the requirements of the *Privacy Act 1988* (**Privacy Act**) and the steps the department is taking to improve its privacy maturity.

1. The frameworks used to identify and manage privacy risks, and meet the requirements of the Privacy Act 1988, in public sector entities that manage information on private individuals

Privacy compliance - policies, governance and oversight

The department's Chief Operating Officer is the agency's designated Privacy Champion. The Privacy Champion is supported by two Privacy Officers and a team of Assistant Privacy Officers. The department's Privacy Officers are the primary point of contact for advice on privacy matters in the department, as well as being the primary point of contact for both the Office of the Australian Information Commissioner (**OAIC**) and members of the public.

As part of its core functions, the department undertakes continuous improvement of its internal processes and procedures. This approach aims to grow and develop the department's privacy maturity on an ongoing basis, with a focus on the identification of opportunities for capability uplift and ensuring internal privacy resources provide clear direction for departmental staff.

Key resources

The department maintains a Privacy Management Plan (**PMP**), which is currently under review. The department also has a comprehensive general Data Breach Response Plan (**general DBR Plan**), which was most recently reviewed and updated in November 2025.

In addition, the department maintains a suite of key resources and templates to assist business areas in ensuring compliance with the requirements of the Privacy Act. These resources include:

- Privacy Notice templates, based on the requirements of Australian Privacy Principle (**APP**) 5;

Australian Government
Department of Health, Disability and Ageing

- protocols/processes for the identification, assessment and, notification of data breaches to the OAIC; and
- Privacy Threshold Assessment (**PTA**) templates and associated guidance around undertaking Privacy Impact Assessments (**PIAs**).

A key part of the department's approach to uplifting privacy capability involves promoting a self-service approach to managing privacy matters where possible. This approach recognises protection of privacy as a collective responsibility and aims to assure the department's privacy maturity across the department.

For example, the department supports its officers in managing privacy through the internal publication of standard operating procedures for:

- dealing with unsolicited personal information (APP 4),
- managing requests for personal information (APP 12), and
- seeking correction of personal information (APP 13).

Most statutory secrecy regimes within Health Portfolio legislation place additional controls on the handling of personal information. As such, the department's key processes and resources relating to the secrecy obligations of its officers also assist in facilitating compliance with the requirements of the Privacy Act.

The department maintains a Privacy Policy[1], a Website Privacy Policy[2] and an Employee Privacy Policy. In addition, a number of departmental programs also have specific privacy policies. These include the National Cancer Screening Program (**NCSP**)[3], My Aged Care[4], Australian Immunisation Register[5] and Electronic Prescribing[6]. The department maintains public-facing Privacy Notices[7] for programs or activities that involve the collection of personal information.

Ensuring third-party compliance with the Privacy Act

The department's contractual templates include clauses to ensure that contracted service providers comply with the APPs, as required by s 95B of the Privacy Act. The template grant agreements also require grantees to comply with the Privacy Act and APPs.

The department is currently developing a suite of additional privacy clauses to include in relevant contracts and grant agreements. These additional clauses aim to enhance the contractual protections established under these contracts and grants. These clauses will impose additional privacy obligations on contracted third parties.

[1] Privacy policy - Department of Health, Disability and Ageing
[2] Website Privacy Policy - Department of Health Disability and Ageing
[3] Privacy Policy - National Cancer Screening Register
[4] Privacy Policy - My Aged Care
[5] Privacy Policy - Australian Immunisation Register
[6] Privacy Policy - Electronic Prescriptions Privacy Policy
[7] See links to departmental Privacy Notices available via the Website Privacy Policy webpage

Australian Government
Department of Health, Disability and Ageing

Data Governance and Risk Management

The department's Risk Management Framework identifies six enterprise risks and associated sub-risks which include legal compliance. Compliance with the Privacy Act sits within this risk category and is subject to a low risk tolerance.

The department's Data Governance Framework[8] sets out the key principles, structures, roles and responsibilities which govern data collection, use, sharing and release activities. In managing personal information held by the department, the department draws on centralised data governance expertise to support consistent and best-practice handling of data. For example, departmental officers have access to technical and practical guidance on the de-identification and confidentialisation of data prior to disclosure to external recipients. This ensures de-identification and confidentialisation processes are underpinned by technical expertise and reflect a best practice approach to the management of privacy risks in the department's data governance framework.

The department also maintains a Data Asset Register. Departmental data stewards are responsible for the management of data assets/information resources listed in the Register. This includes ensuring information resources and data assets are listed in the Data Asset Register and keeping Register entries up to date. The Data Asset Register contains flags for personal or sensitive information and guidance on the legal protections for the information and access protocols.

Coordination across internal business areas and external agencies

The department maintains a series of standing meetings involving its Privacy Law Section and key areas within the department. Participation in these forums facilitates a coordinated approach to identifying and managing emerging privacy issues across business areas responsible for higher volumes of personal information handling.

Legislation and policy development

Significant changes have been made to secrecy regimes in Health Portfolio legislation in recent years, including through the *Regulatory Reform Omnibus Act 2025*. These changes have modernised the secrecy provisions to support the efficient and effective collection, use and disclosure of protected information and assured the protection of individual's sensitive and health information.

Privacy education and training

Training

The department provides mandatory privacy training, which all staff are required to complete on commencement with the department and annually.

The department also provides its officers with targeted privacy training including where the department:

- identifies trends or patterns emerging (such as in the course of regular reviews of its

[8] Data Governance Framework - Department of Health Disability and Ageing

Australian Government
Department of Health, Disability and Ageing

internal data breach register), or
- identifies changes to key processes (for example, processes for the assessment of potential data breaches, or the completion of PTAs).

Other education initiatives

As a supporter of Privacy Awareness Week (PAW), the department develops and participates in PAW activities annually. The department's initiates activities including distributing key messages for all staff with information on privacy obligations (including available resources) and delivering presentations to enhance understanding of privacy principles. In 2026, the department hosted a presentation on what it means to take "reasonable steps" to protect personal information for the purposes APP 11, with a particular focus on data governance and emerging technologies.

The department will be undertaking additional education initiatives to enhance privacy awareness. This will include developing guidance on privacy compliance for officers who have contract management responsibilities and developing FAQs on common or emerging privacy issues.

Data breaches and complaints handling

Data breach frameworks

The department has three key frameworks to manage potential data breaches, comprising:

- the general DBR Plan, and
- separate frameworks specific to the NCSP and the My Aged Care Contact Centre (**MAC CC**).

The NCSP and MAC CC are two areas within the department that manage a large volume of sensitive information. The department has established specific arrangements to support these areas in identifying, managing and escalating data breaches.

The department applies a centrally governed approach to the identification and assessment of potential data breaches, supported by departmental guidance and oversight. All potentially eligible data breaches are reported to the Privacy Law Section. The Privacy Law Section assesses these breaches and, where an eligible data breach is found, facilitates notification to both the OAIC and any affected individuals.

The department handles large volumes of personal and sensitive information and undertakes assessments wherever potential data breaches are identified. The table below sets out the number of notifiable data breaches by financial year since 2022-23.

	2022-23	**2023-24**	**2024-25**	**2025-26 (as at 12 May 2026**
Eligible Data Breaches by financial year	1	8	0	2

Australian Government
Department of Health, Disability and Ageing

Potential eligible data breaches are identified in a number of ways. For example, where an affected individual notifies the department, a contracted service provider or an individual's personal representative notifies the department, or where a departmental officer identifies a potential EDB in the course of their duties.

Potential data breaches involving information included in the National Cancer Screening Register (**NCSR**) are managed under the NCSR Data Breach Response Plan, which sets out:

- the department's approach to managing NCSR data breaches (including maintenance of the NCSR data breach register),
- requirements under section 22A of the *National Cancer Screening Register Act 2016* (**NCSR Act**), and
- relevant information in relation to the department's obligations under the Privacy Act.

Standard Operating Procedures set out processes for managing data breaches and privacy matters relating to the NCSR. Under the NCSR Act, data breaches are reported to the Information Commissioner by the department and Contracted Service Providers (**CSPs**), including former CSPs, on a weekly basis.

Potential data breaches involving the MAC CC are managed in accordance with a Standard Operating Procedure. All potential data breaches are registered on the department's MAC CC Privacy Register and potential eligible data breaches are referred to the Privacy Law Section for assessment. Data breaches assessed as eligible data breaches are reported to the OAIC in accordance with the Notifiable Data Breaches Scheme.

Privacy complaints

The department has a distinct complaint handling process for managing privacy-related complaints. Privacy related complaints received through the department's general enquiries area or by program/policy areas are referred to the Privacy Law Section and are investigated by the department's Privacy Officers.

Analysis and reporting of data breaches, privacy complaints and significant privacy issues

The Privacy Champion receives a quarterly report reflecting the actual and potential eligible data breaches escalated under the general DBR Plan. The Privacy Champion is notified of privacy complaints and eligible data breaches on a case-by-case basis. The Privacy Champion works with the department's Chief Counsel to escalate significant privacy issues to the department's broader Executive.

Separate to this, the MAC CC prepares detailed monthly reports for their Branch Executive on trends/patterns relating to data breaches and remedial action undertaken. In addition, a 'Privacy Multidisciplinary Team' (comprising representatives of each section/team within the relevant branch), meets regularly and prepares reports on lessons learnt and key drivers of data breaches. These reports are routinely shared across the relevant branch to identify areas for improvement.

Australian Government
Department of Health, Disability and Ageing

The Integrity Dashboard provides senior executive leaders (including the Privacy Champion) with a consolidated, quarterly view of the department's integrity performance and emerging risks. It includes data to support oversight, informed decision-making, and continuous improvement in relation to privacy risks. The Dashboard includes metrics relevant to privacy and information handling, such as numbers and causes of potential data breaches and integrity case themes where information misuse is a factor. It is supported by an Insights Paper, which provides further context to the data in the quarterly Dashboard report.

Privacy Impact Assessments

Business areas are responsible for completing PTAs wherever a project involves new or changed ways of handling personal information. This requirement is set out within the intranet resources on PIAs and also discussed in the department's Project Management Framework. The intranet resources regarding PIAs also contain a specific checklist for use when a project involves changes to ICT systems to support a 'privacy by design' approach.

To support this process, the Privacy Law Section maintains a PTA template that provides guidance to the decision-maker. The aim of this guidance is to streamline the assessment process and improve the department's privacy maturity by uplifting expertise across the department more broadly.

Where a project is assessed as high risk, the department engages external legal service providers to undertake a PIA. Once completed, business areas are responsible for implementing PIA recommendations, with support provided by the Privacy Law Section where additional legal advice or guidance is needed.

The AI Use case risk assessment template also prompts the business area to consider if the use case is compliant with the Privacy Act and if a PTA or PIA should be completed. Use cases that raise privacy risks (where a PIA has not been completed) are referred to the Privacy Law Section for advice.

The department has scheduled a review of the new PTA process in the second half of 2026, as part of its continuous improvement processes.

2. The ability of public sector entities holding personal information to respond effectively to data breaches, cyber threats, and malicious actors.

Data breaches

As discussed above, the department has a general DBR Plan and other processes for managing data breaches. The recent changes to the general DBR Plan and decentralisation of the data breach assessment process are designed to uplift capability to identify and respond to data breaches and assist in embedding a privacy positive culture in the department.

Australian Government
Department of Health, Disability and Ageing

Cyber Security – responding to cyber threats and malicious actors

The department has a Security Strategy 2023-26 and a Cyber Security Incident Response Plan (**CSIR Plan**) which defines roles, responsibilities, capabilities and escalation paths during a cyber threat or incident. Under this plan, tasks include determining whether a cyber incident constitutes a data breach under the Privacy Act and supporting any privacy-related assessments with technical facts and expertise.

In accordance with the CSIR Plan, the department undertakes 'tabletop exercises' to test processes and ensure teams are prepared in the event an incident does occur. The department has conducted more than seven internal cyber incident response tabletop exercises to test and validate departmental incident response playbooks.

Additional tabletop exercises are planned with high-risk business areas, with risk prioritisation informed by:

- the sensitivity and volume of data held or managed; and
- the current cyber threat landscape affecting the sector.

The department has also participated in multiple external cyber incident response tabletop exercises, including those coordinated by the National Office of Cyber Security, within the Department of Home Affairs. This included tabletop exercises involving health sector entities (for example, the National Hospital Providers Tabletop in 2025), to support cross-jurisdictional coordination and shared situational awareness.

3. Any matters contained in and associated with Auditor-General Report No. 12 of 2025–26: Managing the Privacy of Client Information in Services Australia.

The department has considered the Auditor-General's report and recommendations.

The department is currently reviewing its Privacy Management Plan, and, in that context, will consider any additional privacy assurance measures including actions to support its maturity assessment outcomes. This review is expected to be completed in mid-2026.

In relation to PIAs, as an additional transparency measure, the department is currently progressing a proposal to publish a description of each PIA on the department's PIA register.