auditoffice
OF NEW SOUTH WALES

Privacy Management Plan

Version: 3.0

Date: 21 October 2026

Review date: October 2027

FROM INSIGHTS TO IMPACT

contents

1.	**Introduction**	**3**
2.	**About the Audit Office**	**3**
3.	**Legislative framework**	**3**
4.	**Implementing and promoting the Plan**	**4**
4.1	Audit Office staff	4
4.2	Public awareness	4
4.3	The Privacy Officer	4
5.	**Policy and procedure development and review**	**5**
6.	**How the Audit Office manages personal and health information**	**5**
6.1	Corporate functions	5
6.2	Referrals to other oversight bodies and integrity agencies	8
6.3	Public interest disclosures	9
6.4	Audit functions	9
7.	**Use of AI**	**11**
8.	**Privacy codes of practice**	**12**
9.	**Public registers**	**12**
10.	**Breaches of the PPIP Act and HRIP Act**	**12**
10.1	Data Breach Management Policy	12
10.2	Offences	13
11.	**Complaints and review rights**	**13**
11.1	Complaints	13
11.2	Internal review	13
11.3	External review by the NSW Civil and Administrative Tribunal (NCAT)	14
11.4	Complaints to the Privacy Commissioner	14
12.	**Contacting the Audit Office**	**15**
13.	**Review**	**15**
Appendix 1: Overview of the IPPs		**16**
Appendix 2: Overview of the HPPs		**19**
Appendix 3: Other applicable laws		**22**

1. Introduction

The Audit Office of New South Wales (the Audit Office) is required by section 33 of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) to have and implement a Privacy Management Plan (the Plan). This Plan includes information on the type of personal and health information the Audit Office holds, details on how people can access their information and what they can do if they think the Audit Office has breached their privacy.

2. About the Audit Office

The Audit Office is a statutory authority established under the *Government Sector Audit Act 1983* (GSA Act) that conducts financial and performance audits of NSW Government agencies, universities and local councils, principally under the GSA Act and the *Local Government Act 1993* (LG Act). These audits help parliament hold government accountable for its use of public resources.

Further information about the Audit Office's functions is contained in our Information Guide.

3. Legislative framework

The PPIP Act sets out the responsibilities of public sector agencies, including the Audit Office, in respect of the management of personal information. It contains 12 Information Protection Principles (IPPs) relating to the collection, storage, access and accuracy, use and disclosure of personal information.

Personal information is defined in section 4 of the PPIP Act and means information or an opinion about an individual whose identity is apparent or can reasonably be ascertained.

Personal information can include a person's name and address, details about their family life, their sexual preferences, financial information, fingerprints and photos. There are some kinds of information that are not personal information, such as information about someone who has been dead for more than 30 years, information about someone that is contained in a publicly available publication, or information or an opinion about a person's suitability for employment as a public-sector official.

The PPIP Act also establishes a mandatory notification of data breach scheme. Section 10.1 of this Plan provides information about how the Audit Office meets the requirements of this scheme.

The *Health Records and Information Privacy Act 2002* (HRIP Act) contains specific provisions about the management of health information and includes a set of Health Privacy Principles (HPPs).

Health information is defined in section 6 of the HRIP Act and can include information about a person's physical or mental health, such as a psychological report, blood test, an X-ray, or information about a person's medical appointment. It can also include personal information that is collected to provide to a health service, such as a name and contact number on a medical record.

Other legislation affecting the way in which the Audit Office manages information includes:

- *Government Sector Audit Act 1983*
- *Local Government Act 1993*
- *Government Information (Public Access) Act 2009*
- *Independent Commission Against Corruption Act 1988*
- *Law Enforcement Conduct Commission Act 2016*
- *Public Interest Disclosures Act 2022*
- *State Records Act 1998*.

Appendix 3 contains additional information about these Acts and related regulations.

4. Implementing and promoting the Plan

The Audit Office reinforces transparency and compliance with the PPIP Act and the HRIP Act by:

- making the Plan publicly available
- ensuring the Plan is regularly reviewed and updated as appropriate
- ensuring associated policies and plans are developed, implemented, and regularly reviewed, including policies on data breach management, records management and information security
- reporting on privacy issues in the Audit Office annual report in accordance with NSW Treasury annual reporting requirements
- undertaking an annual self-assessment of compliance with the PPIP Act
- requiring staff to comply with privacy, secrecy and confidentiality requirements, and embedding this in the Audit Office's Code of Conduct and other relevant policies such as our Grievance Policy
- promoting a culture of good privacy practice
- assessing privacy impacts when introducing or changing systems and processes
- reporting information to the Office Executive and Audit and Risk Committee on privacy breaches.

4.1 Audit Office staff

All Audit Office staff are responsible for ensuring their awareness of and compliance with privacy requirements, policies and procedures.

The Audit Office is committed to making staff aware of and promoting compliance with privacy obligations among staff by:

- publishing the Plan, privacy related policies and other information about privacy on the intranet
- including a reference to the Plan in the onboarding form as part of the induction process and offering training as required
- setting requirements in the data breach management policy for staff to report any suspected breach of privacy or a misuse of personal information
- providing specialist advice and guidance on privacy issues to staff when required, including in relation to privacy impact assessments for changes to systems and processes
- providing updates to staff on changes to privacy requirements and best practice.

4.2 Public awareness

This Plan provides information to members of the public and auditees about how the Audit Office manages personal and health information. The Audit Office promotes public awareness of the Plan by:

- writing the Plan in plain English
- publishing the Plan on the Audit Office website
- referencing the Plan in the Audit Office's Terms of Engagement
- informing people about the Plan when responding to enquiries about personal information.

4.3 The Privacy Officer

The Privacy Officer for the Audit Office is responsible for the Plan and supporting procedures. The Privacy Officer provides advice and guidance to other parts of the Audit Office to support compliance with privacy requirements in their policies, procedures and activities.

The Privacy Officer is the first point of contact when privacy issues arise, either internally or externally, and has responsibility for monitoring the implementation of the Plan and supporting procedures.

Refer to section 12 for how to contact the Privacy Officer.

5. Policy and procedure development and review

In addition to regularly reviewing this Plan, the Audit Office takes the following steps to develop and implement policies and practices that ensure compliance with the PPIP Act and HRIP Act:

- examining changes in the legislative, policy and operational environment for their impacts on the privacy management of the Audit Office
- conducting regular reviews of policies and practices that have privacy implications, including reviews against guidance published by the Information and Privacy Commission (IPC)
- considering the privacy impacts of changes to policies, practices and systems
- notifying staff of changes to policies and practices, and consulting with staff, where appropriate.

Audit Office staff can access related policies and procedures on the 'Policies, forms & templates' intranet page, or through visiting topic-specific intranet pages (e.g., on Privacy management or Information management and security).

The Audit Office publishes policy documents which are likely to impact members of the public on our website.

6. How the Audit Office manages personal and health information

This section of the Plan provides information about how the Audit Office manages personal and health information in the context of:

- corporate functions (section 6.1)
- referrals to and from other oversight bodies and integrity agencies (section 6.2)
- public interest disclosures (section 6.3)
- audit functions (section 6.4).

Appendices 1 and 2 provide a summary of the IPPs and HPPs, and how they apply to the Audit Office, including where exemptions or exceptions may apply.

6.1 Corporate functions

Collection

When collecting personal and health information, the Audit Office take reasonable steps to ensure:

- we do not collect more than we need
- the person understands why the information is being collected and what it will be used for
- what we collect is accurate and relevant to the purpose we are collecting it for, and
- we do not unreasonably intrude into the personal affairs of the relevant person.

The Audit Office provides information to individuals about how their information is collected and used through this Plan, information on our website and through direct communication with individuals.

Information may be received:

- over the phone (including a voicemail service)
- in writing (e-mail, letter, online form)
- in person (at our Office premises and at events).

The Audit Office generally retains a full copy of information received in writing, and a record of information provided over the phone or in person.

The Audit Office collects **personal information** for a range of purposes relevant to our corporate functions, including:

- recruitment information to enable the processing of employment applications (the Audit Office's Employment Screening Policy provides further information)
- staff information to
  - manage ongoing employment relationships, such as maintaining employee records, managing employees and their performance, and administering salary and superannuation
  - manage employee code of conduct requirements, including information for registers relating to conflicts of interest, gifts and benefits, and secondary employment and volunteering
- visitor information for workplace health and safety purposes (names and contact details)
- information for mailing lists (names and contact details)
- information relating to stakeholder engagement, including events and training facilitated by the Audit Office
- information for auditee and parliamentary surveys (name and contact details, position, organisation details)
- information in GIPA Act access applications and requests for information (name, contact details and other personal information specific to a particular matter)
- information about third parties to manage supply engagements or contractual arrangements
- information in general correspondence and enquiries sent to the Audit Office
- information in complaints and feedback about the Audit Office (refer to the Audit Office's Complaints Management Policy for further information).

In most circumstances personal information is collected directly from the individual. Examples of this include information in the online recruitment application and in the onboarding form, or medical information submitted by an individual as part of a personal leave application.

In some circumstances information may be collected from third parties with the consent of the individual. For example, for recruitment purposes information may be collected from third-party recruitment providers, previous employers and nominated referees.

Occasionally, the Audit Office will receive information from other integrity agencies, including when referred to the Audit Office in accordance with a Memoranda of Understanding. See section 6.2 of this Plan for further information.

The Audit Office generally does not collect **health information** for our corporate functions other than for the purposes of workforce management, such as:

- medical certificates to support personal leave requests
- health declarations showing medical conditions relevant to workplace adjustments
- fitness for duty assessments[1]
- workers compensation records.

Refer to Appendix 2 for further information about how the HPPs apply.

Anonymous feedback and reports

The Audit Office recognises that there may be circumstances when people may wish to remain anonymous when providing feedback or reporting information to the Audit Office. The provision of personal information is entirely voluntary. The Audit Office may be limited in how it can deal with information received anonymously.

[1] Note: Fitness for duty assessments are conducted by an independent medical assessor. The affected employee is aware that the assessor provides a report to the Audit Office and also receives a copy. The information in the report is treated in accordance with the PPIP Act and the HRIP Act.

Unsolicited information

The Audit Office limits the collection of personal and health information to that which is reasonably necessary to deal with each enquiry. For example, the Audit Office is not a complaints-handling agency and aims to respond to misdirected complaints promptly to avoid additional information being provided to the Audit Office unnecessarily.

From time-to-time, the Audit Office receives correspondence that contains unsolicited personal and/or health information. For example, if a member of the public provides information to the Audit Office that is not relevant to our functions or has not been asked for. Collection obligations do not apply to 'unsolicited information' (PPIP Act section 4(5) and HRIP Act section 10). The Audit Office has established a formal procedure for managing unsolicited personal or health information received from public correspondence, ensuring that such information is handled and disposed of lawfully and consistently.

If the Audit Office needs to retain the unsolicited information to deal with the individual's enquiry, the information will be managed in accordance with the IPPs and HPPs relating to the storage, use and disclosure of information.

Website privacy statement

Visits to the Audit Office's website do not result in a collection of any personally identifiable information. Further details about the types of information collected about visits to the Audit Office website can be accessed here.

Storage and security

The Audit Office has a range of information management and security policies in place to ensure that personal and health information is stored, retained and disposed of appropriately. These policies and related procedures and controls aim to ensure that personal and health information:

- is kept for no longer than is necessary for the purposes for which the information may lawfully be used
- is disposed of securely and in accordance with any requirements for the retention and disposal of the information, including under the *State Records Act 1998* and related retention and disposal authorities
- is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse.

Most personal and health information collected or held by the Audit Office is stored electronically in systems maintained with the Audit Office's secure IT environment. Before storing information in new locations, the Audit Office may complete, where relevant a privacy impact assessment.

The Audit Office records management system contains restrictions and controls to make sure that personal and health information stored electronically can only be accessed by authorised staff. For example, staff personnel files can only be accessed by relevant staff within the Audit Office's People & Culture function, and is available to direct managers on an as needs basis.

Audit Office policies and procedures for record-keeping and information management are developed in line with requirements in the *State Records Act 1998*, ISO/IEC 27001:2022 (Information security, cybersecurity and privacy protection) and the NSW Government Information Classification, Labelling and Handling Guidelines.

The Audit Office also has policies and procedures to ensure that information provided to third parties in connection with the provision of a service to the Audit Office (e.g., Audit Service Providers, consultants and contractors) is managed securely and is protected from unauthorised use or disclosure of the information. When engaging a third party, privacy obligations are included in contractual arrangements.

The Audit Office does not typically store personal and health information in hard copy files. Where this is necessary, the information is stored securely to ensure that access is limited only to relevant staff, including through a 'clean desk' policy meaning hard copy files are secured at the end of the day and when not in use.

Access and accuracy

The Audit Office's Privacy Officer can help you understand whether the Audit Office holds information about you, the nature of this information, the purpose for which it is used and your rights to access or amend your information.

The Audit Office is required to provide you with access to the personal and health information it holds about you, and to allow necessary amendments to your information, without excessive delay or expense, unless an exemption applies. There is no fee to access or amend personal or health information.

The PPIP Act and the HRIP Act generally do not give people the right to access or amend someone else's information, but you may be able to request this with the other person's consent.

You may also have the right to make a formal application to access information under the *Government Information (Public Access) Act 2009*. For more information, please refer to the IPC website.

Use

The Audit Office takes reasonable steps to check that the information it collects is relevant, accurate, up to date, complete and not misleading before using the information.

The Audit Office only uses personal and health information for purposes directly related to the collection of the information, unless the individual has consented to another use, or where the use is otherwise permitted under the PPIP Act or HRIP Act (e.g., to prevent a serious threat to the health or welfare of an individual).

Disclosure

The Audit Office only discloses personal and health information for purposes directly related to the collection of the information, unless the individual has consented to another disclosure, or disclosure is otherwise permitted under the PPIP Act or HRIP Act (e.g., to prevent a serious threat to the health or welfare of an individual), or other legislation (e.g., see section 6.2 below on referrals to integrity agencies).

The Audit Office may disclose information about its staff to third party service providers that support the Audit Office's workforce management.

The Audit Office does not disclose, without consent, sensitive personal information, such as ethnicity or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities, or trade union membership.

The Audit Office's Code of Conduct requires staff to manage all information owned, received and held by the Audit Office in a secure manner. Staff must maintain the confidentiality and security of all official information, including personal information. This obligation continues after staff have left their employment at the Audit Office.

6.2 Referrals to other oversight bodies and integrity agencies

Although the Audit Office is not a complaints-handling agency, we sometimes receive complaints from public officials or members of the public about the entities we audit. To the extent such information is relevant to our audit functions, the Audit Office may use this information to inform our audits or future audit planning and topic selection.

The Audit Office also has a Memorandum of Understanding with the NSW Ombudsman and a Memorandum of Understanding with the Office of Local Government to cover the referral and sharing of information from complaints made by public officials and from members of the public.

Both memoranda provide for confidentiality and only allow for the sharing of personal information without consent of the reporter/ complainant in certain circumstances, i.e., when 'reasonably necessary' to assist the other agency in carrying out its functions *and* consistent with any other permissions under relevant legislative frameworks. The memoranda also state that express consent is required for the sharing of sensitive personal information, such the complainant's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities.

In some cases, the Audit Office may be required to refer information to another agency (this may apply to information relating to our corporate or audit functions). For example, the Audit Office is required to report possible corrupt conduct to the Independent Commission Against Corruption (ICAC) and the ICAC can issue a notice under sections 21 to 23 of the *Independent Commission Against Corruption Act 1988* requiring that the Audit Office provides information.

Other situations may arise where the Audit Office is legally required to disclose personal or health information.

The principles and approaches in these memoranda are applied by the Audit Office to referrals to other integrity agencies insofar as they are also consistent with any specific referral requirements that apply (e.g., under the ICAC Act).

6.3 Public interest disclosures

The Audit Office may receive public interest disclosures (PIDs) from public officials reporting wrongdoing under the *Public Interest Disclosures Act 2022* (PID Act).

Information about an individual that is contained in a PID within the meaning of the PID Act, or that has been collected while dealing with a PID under the PID Act, does not constitute 'personal information' or 'health information' for the purposes of the PPIP Act and HRIP Act (section 4(3)(e) of the PPIP Act and section 5(3)(h) of the HRIP Act). This means that the IPPs or HPPs do not apply to enable the PID to be dealt with under the PID Act.

The Audit Office complies with section 64 of the PID Act, which prevents the disclosure of identifying information about a reporter without their consent or in limited other circumstances.

Information about how to make a PID to the Audit Office and our policies for dealing with PIDs can be found on our website.

6.4 Audit functions

The Audit Office manages personal and health information collected during audit functions consistent with the IPPs and HPPs, unless an exemption applies.

Collection

The Audit Office is entitled to 'free and full' access to information for our audit purposes under section 36 of the GSA Act and section 423 of the LG Act. This entitlement exists despite any duty of secrecy or other restriction on disclosure that may apply. This enables the Audit Office to access information (including personal and health information where necessary) from auditable entities and related entities for our audit purposes.

Personal information

The types of personal information collected during the audit process may include names, contact details, payroll information, employment details and details of contractual arrangements.

The exemption in section 27A(b)(iii) of the PPIP Act means that the Audit Office is not required to comply with the IPPs relating to the collection, use or disclosure of personal information if:

- the Audit Office is being provided with information from, or is providing information to, another public sector agency, and

- the collection, use or disclosure of the information is reasonably necessary to enable the auditing of the accounts or performance of a public sector agency or agencies.

The PPIP Act defines 'public sector agency' as including an auditable entity or any other entity within the meaning of the GSA Act. For performance audits, this may include a non-public sector entity that receives money or resources, whether indirectly or directly, from or on behalf of a state government entity for a particular purpose or from or on behalf of a local government entity for a local government purpose (a relevant entity under Part 3 Division 2A of the GSA Act and section 136 of the LG Act).

The Audit Office may also collect and manage personal information relating to stakeholders or, in limited circumstances, members of the public, during our audits. For example, the Audit Office may receive personal information in public submissions relating to a performance audit or when organising and conducting interviews with members of the public.

Unless an exemption applies, personal information is collected by the Audit Office during audit functions in accordance with the IPPs (see Appendix 1 for further information).

Health information

The Audit Office does not routinely collect or use health information for our audit work.

In limited circumstances, health information may be collected from a public sector agency or directly from individual stakeholders during a performance audit. The Audit Office only collects health information that is reasonably necessary for the purposes of the audit. For example, where this is necessary to assess the effectiveness of a health service program.

It is not reasonably practicable for the Audit Office to notify individuals when it is collects health information from a public sector agency for audit purposes, and the secrecy requirements prevent this (see Disclosure section below). De-identified information will be collected from entities where reasonably practicable.

Where health information is collected directly from an individual for audit purposes, the Audit Office takes reasonably steps to inform the individual about why their information is being collected and how it will be used. We also take reasonable steps to ensure the information collected is relevant to the audit purpose, is not excessive and is accurate, up to date and complete, and does not unreasonably intrude on the individual's personal affairs.

Storage and security

The Audit Office manages information collected during an audit in secure information management systems with specific controls to ensure access is appropriately limited to relevant Audit Office staff or contractors on a needs-to-know basis.

Section 6.1 of this Plan provides further information about how the Audit Office manages the storage and security of information.

Access and accuracy

Section 6.1 of this Plan provides information about how an individual can request access to or the amendment of personal or health information that the Audit Office has collected from the individual.

Any person wishing to access or amend personal or health information which has been obtained from an agency as part of the Audit Office's audit functions should contact the agency that provided the information to the Audit Office. This is because secrecy requirements prevent the Audit Office from disclosing matters that come to our knowledge during the exercise of audit functions (see Disclosure section below for further information).

Use

Personal information collected during the audit process is only used for the purpose of the audit. Our audit files (which may contain personal information) may be reviewed during independent reviews of our work. Where our work is reviewed by a third party, they are bound by the same privacy principles as the Audit Office.

Disclosure

The Audit Office is required under section 38 of the GSA Act and section 425 of the LG Act to preserve the secrecy of all information obtained whilst undertaking audit work. Sections 38(2) of the GSA Act and 425(2) of the LG Act contain exceptions to the requirements of the secrecy provisions (e.g., the secrecy provisions do not apply where disciplinary proceedings are taken against a public official).

Generally, audit teams will not include personal or health information in audit products provided to audited entities, even if these are not intended for publication. Neither personal nor health information should be included in any of the Audit Office's published reports.

There are some limited situations where the Audit Office may be required to disclose information collected during an audit, which may include personal or health information. For example, the Audit Office is required to report possible corrupt conduct to the Independent Commission Against Corruption and the ICAC can issue a notice under sections 21 to 23 of the ICAC Act requiring that the Audit Office provides information. Other situations may arise where the Audit Office is legally required to disclose personal or health information.

In addition to the secrecy requirements of the GSA Act and LG Act, the Accounting Professional and Ethical Standards Board's (APESB) APES 110 Code of Ethics for Professional Accountants (including Independence Standards) imposes an ethical requirement on professional accountants to respect the confidentiality of information acquired as a result of professional and business relationships, not to disclose any such information to third parties without proper and specific authority, unless there is a legal or professional right or duty to disclose and not to use the information for the personal advantage of the APESB member or third parties.

7. Use of AI

The Audit Office's Use of Artificial Intelligence Policy aims to ensure that the confidentiality of Audit Office information is protected and that we have guardrails in place for safe, appropriate and responsible use of approved AI.

The Audit Office's staff may use approved AI tools to support administrative tasks, planning, research and analysis where this is consistent with the Use of Artificial Intelligence Policy and the related guardrails established by the Audit Office.

Audit Office staff must not use non-approved AI tools (including public AI tools) to upload or analyse non-public Audit Office information (including personal information).

Controls are implemented to ensure the security of information used in approved AI tools, including to ensure information remains within the Audit Office's secure IT environment, and to prevent the unauthorised access or disclosure of information. This includes controls to ensure that approved AI tools are not trained using Audit Office information in a way that could result in external disclosure of Audit Office information.

Audit Office staff must not use AI tools to input or analyse personal information collected for non-audit purposes, for example corporate, people and culture, or administrative purposes.

The Audit Office does not use automated decision-making systems to make decisions about our staff or the people we deal with.

Audit functions

Audit Office staff may use personal information in approved AI tools to support activities that are reasonably necessary to enable the auditing of the accounts or performance of a public sector agency or group of public sector agencies. For example, searching, summarising, analysing, extracting or classifying information collected from another agency that contains personal information (e.g., payroll datasets, interview data). Where reasonably practicable, staff should use de-identified personal information before collecting, using and/or storing the information if the inclusion of personal information is not required for an audit or assurance activity.

8. Privacy codes of practice

Under the PPIP Act, a privacy code of practice may regulate the collection, use and disclosure of, and the procedures for dealing with, personal information held by public sector agencies.

Under the HRIP Act, Health Privacy Codes of Practice can be made by an agency or the Privacy Commissioner to modify the application of one or more HPPs or the provisions for the private sector.

These Codes are available on the IPC website. Currently, there are no Codes of Practice that affect how the Audit Office manages personal or health information.

9. Public registers

Part 6 of the PPIP Act governs how NSW public sector agencies should manage personal information contained in public registers. The Audit Office maintains the following public registers that can include personal information:

- Gifts, benefits and hospitality registers
- Act of Grace payment registers
- Gifts of Government property registers.

Individuals who have personal information contained in a public register can contact the Privacy Officer with inquiries about how to request access to or suppression of personal information in a public register. Section 12 explains how to contact the Privacy Officer.

10. Breaches of the PPIP Act and HRIP Act

All Audit Office staff are responsible for ensuring their awareness of and compliance with privacy policies and procedures. Any suspected breach of privacy or a misuse of personal information must be immediately reported to the Privacy Officer or appropriate people manager. Breach of the Audit Office's privacy policies may result in disciplinary action. Public sector employees may be fined or imprisoned for misusing personal information under the PPIP Act and the HRIP Act.

10.1 Data Breach Management Policy

The PPIP Act also establishes a mandatory notification of data breach (MNDB) scheme. This includes a requirement for the Audit Office to publish a data breach management policy.

The Audit Office's Data Breach Management Policy provides guidance to staff on managing data breaches, including those involving personal information and those where mandatory notifications are required. Data breaches may also involve breaches of provisions in the PIPP Act or HRIP Act.

The Data Breach Management Policy sets out five steps for responding to and reporting data breaches.

When a potential data breach is identified, the Audit Office will promptly contain the breach and assess its nature and severity. Any breach that involves personal information is assessed to consider whether there is a likely risk of serious harm to the individuals affected and is thereby an 'eligible data breach'. This assessment is approved by the Deputy Auditor-Geneal on the advice of the Privacy Officer.

Under the policy, where an eligible data breach has occurred, the Deputy Auditor-General notifies the Privacy Commissioner immediately using the required form and affected individuals as soon as practicable. The policy provides more details on these processes, including about how and when to notify affected individuals, and the procedures for public notices if individuals cannot be contacted.

The Audit Office has an internal register to capture and report on data breaches and respond to those incidents, including 'eligible data breaches' as required under the PPIP Act.

The Audit Office also publishes the Data Breach Management Policy and public notifications register on our website.

10.2 Offences

The PPIP Act and HRIP Act create offences for corrupt and improper misuse of personal information or health information.

In summary:

- a public sector official must not intentionally disclose or use personal or health information about an individual to which the official has or had access to in the exercise of his or her official functions, otherwise than in connection with the lawful exercise of their official functions
- a person must not induce or attempt to induce a public sector official (by way of a bribe or other similar corrupt conduct) to disclose any personal or health information about another person to which the official has or has had access in the exercise of his or her official functions
- a person must not offer to supply personal or health information that has been disclosed unlawfully
- a person must not hinder the Privacy Commissioner or a staff member from doing their job.

Under the HRIP Act specifically:

- a person must not, by threat, intimidation, or false representation, attempt to persuade an individual to refrain from making or to withdraw an application pursuing a request for access to health information or a complaint to the Privacy Commissioner or NCAT
- a person must not by threat, intimidation, or false representation require another person to give consent or to do, without consent, an act for which consent is required.

11. Complaints and review rights

11.1 Complaints

If an individual has a complaint about how the Audit Office has dealt with their personal and health information, they can seek to resolve the matter informally by contacting the Privacy Officer with the details of the complaint. Information about how to make a complaint about the Audit Office and a copy of the Complaints Management Policy are available on the Audit Office website.

11.2 Internal review

If a person feels aggrieved by the conduct of the Audit Office in respect of a privacy issue, they are entitled to an internal review under the PPIP Act. An application for internal review must:

- be in writing
- be addressed to the Audit Office of New South Wales
- include a return address for correspondence
- be lodged within six months of the date the applicant first became aware of the conduct.

The Audit Office may accept an internal review application lodged more than six months after the applicant first became aware of the conduct subject to the complaint (a late application). The Audit Office

will consider the circumstances of the delay, including any explanation provided by the applicant. If the Audit Office decides not to accept a late application, reasons will be provided to the applicant.

An internal review can be requested by filling out the internal review form available on the Information and Privacy Commission New South Wales (IPC) website. It is not compulsory to complete the form, however an internal review must be requested in writing.

The review will be conducted by either:

- the Privacy Officer, or
- another member of staff if the Privacy Office was substantially involved in any matter relating to the conduct subject of the complaint or is unable to conduct the internal review.

The Audit Office will following our Privacy Internal Review Procedure to conduct the review. The Audit Office will also refer to the NSW Privacy Commissioner's (Privacy Commissioner) materials available on the IPC website, in particular the privacy internal review checklist and guidance how to handle an internal review. The Audit Office will acknowledge receipt of a request for an internal review within seven days and complete the internal review within 60 days. The Audit Office will keep the applicant up to date with the progress of the internal review and will advise as soon as practicable if the review is likely to take more than 60 days.

Within 14 days of completing the review, the Audit Office will notify the applicant in writing about the findings of the review, the actions the Audit Office proposes to take and their right to further review.

As required by the PPIP Act, the Audit Office will:

- notify the Privacy Commissioner of an application for internal review
- keep the Privacy Commissioner informed of the progress of the review
- inform the Privacy Commissioner of the findings of the review and the action proposed to be taken in relation to the matter.

The Privacy Commissioner can make submissions to the Audit Office in relation to the subject matter of the application for internal review.

11.3 External review by the NSW Civil and Administrative Tribunal (NCAT)

If the Audit Office has not completed the internal review within 60 days, the applicant disagrees with the findings of the internal review or is not satisfied with the action taken by the Audit Office in relation to the application, the applicant has the right to apply to the NCAT for an external review of the conduct.

Further information about making an application to the NCAT can be found on the NCAT website.

The NCAT can be contacted at:

Phone: 1300 006 228
Post: Level 9, John Maddison Tower, 86-90 Goulburn Street, SYDNEY NSW 2000

11.4 Complaints to the Privacy Commissioner

An individual can make a complaint to the Privacy Commissioner about a breach of their privacy by the Audit Office. More information about the role of the IPC in handling complaints, including the contact details, can be found on the IPC website.

The IPC can be contacted at:

Email: ipcinfo@ipc.nsw.gov.au
Phone: 1800 472 679
Post: GPO Box 7011 SYDNEY NSW 2001

12. Contacting the Audit Office

For more information about this Plan or about the personal information the Audit Office holds, please contact the Privacy Officer:

Email: governance@audit.nsw.gov.au
Phone: 02 9275 7100
Post: GPO Box 12, SYDNEY NSW 2001

13. Review

The Plan will be reviewed annually, or more frequently if required, taking into account significant legislative or organisational changes, risk factors and consistency with other policies. The next review is due in October 2027.

Document information

Title:	Privacy Management Plan
Owner:	Governance
Person responsible:	Director, Legislation & Assurance
Approver:	Executive Director, Quality, Improvement and Performance
Last updated:	21/10/2026
Next review date:	10/2027
Document reference:	R012-1761212392-33133

Document history

Version	Date	Reason for Amendment
3.0	October 2026	Review and restructure to improve accessibility and completeness. Additional content relating to the use of AI.
2.4	June 2025	Biannual review and update.
2.3	February 2024	Biannual review and update. Additional content to reflect requirements of the NSW Mandatory Notification of Data Breach Scheme and other relevant legislative amendments.
2.2	August 2022	Biannual review and update.
2.1	March 2020	Minor amendments made following receipt of feedback from the IPC.
2.0	March 2020	Biannual review and update, including formatting change.
1.4	February 2018	Minor amendments made following an assessment of the Plan against the IPC Checklist for review of Privacy Management Plans.
1.3	January 2018	Biannual review and update.
1.2	May 2016	Annual review and update.
1.1	March 2015	Annual review and update.
1.0	July 2014	Privacy Management Plan document developed.

Appendix 1: Overview of the IPPs

Part 2, Division 1 of the PPIP Act contains 12 Information Protection Principles (IPPs) that the Audit Office must comply with in the exercise of our functions, unless an exemption applies.

An exemption applies to certain privacy principles (specifically, those relating to collection (IPPs 1-4), use (IPPs 9-10) and disclosure (IPPs 11-12)) in the context of personal information exchange between public sector agencies for audit purposes. Other potentially relevant exemptions under the PPIP Act are listed at the end of this Appendix.

Below is an overview of the IPPs as they typically apply to the Audit Office, including information about exemptions that may apply. Refer to section 6 of this Plan for further information.

Summary of IPP	Audit Office application
Collection	
IPP 1 – Lawful An agency must only collect personal information for a lawful purpose, which is directly related to the agency's function or activities and is reasonably necessary for that purpose. An agency must not collect personal information by any unlawful means.	The Audit Office collects personal information only for a lawful purpose that is directly related to the Audit Office's functions and activities, and that is reasonably necessary for that purpose.
IPP 2 – Direct In collecting personal information, an agency must only collect personal information directly from the person concerned, unless they have authorised collection from someone else, or if the person is under 16 and the information has been provided by a parent or guardian.	The Audit Office collects personal information directly from the person concerned, unless they have authorised collection from someone else. **The Audit Office is not required to comply with IPP 2 if the collection from a public sector agency is reasonably necessary to enable our audit functions.**
IPP 3 – Open An agency must take reasonable steps to inform the person they are collecting the information from why they are collecting it, what they will do with it and who else might see it. The agency must also tell the person how they can view and correct their personal information, if the information is required by law or voluntary, and any consequences that may apply if they decide not to provide their information.	The Audit Office informs people why their personal information is being collected, what it will be used for, and to whom it will be disclosed. The Audit Office will tell people how they can access and amend their personal information and any possible consequences if they decide not to give their personal information to the Audit Office. **The Audit Office is not required to comply with IPP 3 if the collection from a public sector agency is reasonably necessary to enable our audit functions.**
IPP 4 – Relevant An agency must take reasonable steps to ensure that the personal information collected is relevant, accurate, complete, up-to-date and not excessive and that the collection does not unreasonably intrude into the personal affairs of the individual.	The Audit Office takes reasonable steps to ensure the personal information it collects from individuals is relevant, accurate, not excessive and does not unreasonably intrude into the personal affairs of the individual. **The Audit Office is not required to comply with IPP 4 if the collection from a public sector agency is reasonably necessary to enable our audit functions.**
Storage	
IPP 5 – Secure An agency must store personal information securely, keep it no longer than necessary for the purposes it was lawfully collected and disposes of it appropriately. The personal information should also be protected from loss, unauthorised access, use, modification or disclosure.	The Audit Office stores personal information securely, keeps it no longer than necessary and disposes of it appropriately. Personal information is protected from unauthorised access, use, modification or disclosure. **IPP 5 applies to all personal information held by the Audit Office.**

Summary of IPP	Audit Office application
Access and accuracy	
IPP 6 – Transparent An agency must take reasonable steps to explain to the person what personal information about them is being stored, why it is being stored and any rights they have to access it.	The Audit Office takes reasonable steps to explain to individuals what personal information about them is being stored, what it is used for and the right to access and amend it, unless an exemption applies. For example, an exemption to IPP6 may apply to information collected from a third party during our audits due to the secrecy requirements that apply to audit information (see section 25 of the PPIP Act and Appendix 3).
IPP 7 – Accessible An agency must at the request of the individual to whom the information relates allow the individual to access their personal information without excessive delay or expense.	The Audit Office allows people to access their personal information without unreasonable delay or expense, unless an exemption applies. For example, an exemption may apply in relation to information collected from a third party during our audits due to the secrecy requirements that apply to audit information (see section 25 of the PPIP Act and Appendix 3).
IPP 8 – Alteration An agency must at the request of the individual to whom the information relates, allow them unless an exception applies, to make appropriate amendments either by way of update, correction, or amendment to their personal information where necessary to ensure that the personal information is accurate, relevant, up to date, complete and not misleading when considering the purpose for which it is to be used.	The Audit Office allows people to update, correct, or amend their personal information where necessary. For example, an exemption may apply in relation to information collected from a third party during our audits due to the secrecy requirements that apply to audit information (see section 25 of the PPIP Act and Appendix 3).
Use	
IPP 9 – Accurate An agency must take reasonable steps to ensure that the personal information is relevant, accurate, up to date and complete before using it.	The Audit Office takes reasonable steps to ensure that personal information is relevant, accurate and complete before using it. **The Audit Office is not required to comply with IPP 9 if the use of information collected from or provided to a public sector agency is reasonably necessary to enable our audit functions.**
IPP 10 – Limited An agency must only use personal information for the purpose it was collected unless the person has given their consent, or the purpose of use is directly related to the purpose for which it was collected, or to prevent or lessen a serious or imminent threat to any person's health or safety.	The Audit Office only uses personal information for the purpose it was collected for unless the person consents to another use, or the purpose of use is directly related to the purpose for which it was collected, or to prevent or lessen a serious or imminent threat to any person's health or safety. **The Audit Office is not required to comply with IPP 10 if the use of information collected from or provided to a public sector agency is reasonably necessary to enable our audit functions.**

Summary of IPP	Audit Office application
Disclosure	
IPP 11 – Restricted An agency can only disclose personal information in limited circumstances with a person's consent or if the person was told at the time when the personal information was collected it that it would be disclosed. An agency can also disclose personal information if disclosure is directly related to the purpose for which the information was collected and there is no reason to believe the person would object, or the person has been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.	The Audit Office will only disclose personal information with people's consent or for a purpose directly related to its collection. In some circumstances, disclosure may be required or permitted by law without the individual's consent (see section 6.2 of this Plan). **The Audit Office is not required to comply with IPP 11 if the disclosure of information collected from or provided to a public sector agency is reasonably necessary to enable our audit functions. However, secrecy requirements apply to information obtained during our audits which means the information may only be disclosed in limited circumstances (see Appendix 3 for further information).**
IPP 12 – Safeguarded An agency cannot disclose certain categories of personal information without a person's consent. Those categories include information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. It can only disclose these categories of personal information without consent if the disclosure is necessary to prevent a serious and imminent threat to any person's health or safety.	The Audit Office does not disclose, without consent, sensitive personal information, such as ethnicity or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities, or trade union membership. **The Audit Office is not required to comply with IPP 12 if the disclosure of information collected from or provided to a public sector agency is reasonably necessary to enable our audit functions. Generally, we do not collect sensitive personal information as part of our audit functions.**

Other exemptions

Other exemptions in the PPIP Act that may apply to the Audit Office's collection and management of personal information depending on the circumstances include:

- exemptions relating to law enforcement and related matters (section 23)
- exemptions relating to assisting another public sector agency that is an investigative agency in exercising its investigative functions (section 24)
- exemptions where non-compliance is lawfully authorised or required (section 25)
- exemptions where non-compliance would benefit the individual concerned (section 26)
- exemptions relating to emergency situations (section 27D)
- exemptions relating to disclosures of information for the purposes of informing the relevant Minister or the Premier about matters (section 28).

Appendix 2: Overview of the HPPs

Schedule 1 of the HRIP Act contains 15 Health Privacy Principles (HPPs) that the Audit Office must comply with, unless an exception applies. Unlike for personal information, there is no general exemption to the application of certain HPPs in the context of information exchanged for audit purposes. Exceptions are therefore considered on a case-by-case basis.

The below table provides an overview of the HPPs as they apply to the Audit Office, including where exceptions may apply. Refer to section 6 of this Plan for further information.

Summary of HPP	Audit Office application
Collection	
HPP 1 – Lawful An organisation must only collect health information for a lawful purpose that is directly related to the agency or organisation's activities and necessary for that purpose. Health information should not be collected by any unlawful means.	The Audit Office collects health information only for lawful purposes that are directly related to the Audit Office's functions and activities and necessary for that purpose. **Note: there are no exceptions to this HPP.**
HPP 2 – Relevant An organisation that collects health information from an individual must take reasonable steps to ensure that the information collected is relevant, accurate, up to date, complete and not excessive, and that the collection does not unreasonably intrude into the personal affairs of the person to whom the information relates to.	When collecting information from an individual, the Audit Office takes reasonable steps to ensure that the information collected is relevant, accurate, complete and not excessive, and that the collection does not unreasonably intrude into the personal affairs of the person to whom the information relates. **Note: there are no exceptions to this HPP.**
HPP 3 – Direct An organisation must only collect health information from the person concerned, unless it is unreasonable or impracticable to do so.	The Audit Office collects health information directly from the person concerned, unless it is unreasonable or impracticable to do so. For example, in limited circumstances, the Audit Office may collect health information for audit purposes from public sector agencies where it is unreasonable or impracticable to collect the information from the person(s) concerned.
HPP 4 – Open An organisation that collects health information about an individual from the individual must at or before the time (or if not practicable as soon as practicable after that time) that it collects the information take reasonable steps to inform the person the identity of the organisation collecting the information and how to contact it, the fact that the individual is able to request access to the information, why they are collecting their health information, what they will do with it, and who else may see it. An organisation is to inform the individual of any law that requires the collection and of any consequences that will occur if they decide not to provide their information to the organisation. If an organisation collects health information about a person from a third party, it must still take reasonable steps to notify the person that this has occurred.	When collecting health information from individuals, the Audit Office informs people why their information is being collected, what it will be used for and to whom it will be disclosed. We will tell people how they can access and amend their health information and any possible consequences if they decide not to give their health information to the Audit Office. The Audit Office will inform an individual of any law that requires the collection and of any consequences if they decide not to provide their information. If the Audit Office collects health information about a person from a third party, the Audit Office will take reasonable steps to notify the person that this has occurred and how their information will be used. Generally, individuals will not be notified where health information is collected for our audit functions from a public sector agency because this would not be reasonably practicable, and secrecy requirements apply to information obtained during our audits.

Summary of HPP	Audit Office application
Storage	
HPP 5 – Secure An organisation that holds health information must ensure the health information is stored securely, not kept any longer than necessary for the purposes of its collection, and disposed of appropriately. An organisation is to ensure that appropriate security safeguards as are reasonable in the circumstances are in place, so that the health information is protected against loss, unauthorised access, use, modification, disclosure or any other misuse.	The Audit Office stores health information securely, keeps it no longer than necessary and disposes of it appropriately. Health information is protected from unauthorised access, use, modification, disclosure or any other misuse through appropriate security safeguards. **Note: there are no exceptions to this HPP.**
Access and accuracy	
HPP 6 – Transparent An organisation that holds health information must take reasonable steps to explain to the person whether health information is held, whether it holds health information relating to that person and if health information is held what health information is being stored, the reasons it is being used and any rights they have to access it.	The Audit Office takes reasonable steps to explain to individuals what health information about them is being stored, what the information is used for and the right to access and amend it, **unless an exception applies** (e.g., where compliance with HPP 6 would result in a breach of the secrecy requirements that apply to information obtained during our audits).
HPP 7 – Accessible An organisation that holds health information must allow a person to access their health information without unreasonable delay or expense.	The Audit Office allows people to access their own health information without unreasonable delay or expense, **unless an exception applies** (e.g., where compliance with HPP 7 would result in a breach of the secrecy requirements that apply to information obtained during our audits).
HPP 8 – Correct An organisation is to allow a person to whom the information relates, to update, correct, delete, add or amend their health information where necessary (unless an exception applies) to ensure that the health information is accurate, is being collected or used for its directly related purpose, and is relevant, up to date, complete and not misleading.	The Audit Office allows people to update, correct, or amend their health information where necessary, **unless an exception applies** (e.g., where compliance with HPP 8 would result in a breach of the secrecy requirements that apply to information obtained during our audits).
HPP 9 – Accurate An organisation that holds health information must not use the health information without having taken reasonable steps to ensure that it is relevant, up to date, accurate, complete, and not misleading.	The Audit Office takes reasonable steps to ensure the health information is relevant, up to date, accurate, complete and not misleading before using it. **Note: there are no exceptions to this HPP.**
Use	
HPP 10 – Limited An organisation that holds health information must only use health information for the purpose for which it was collected or for a directly related purpose, which a person would expect. Otherwise, use of the health information for a secondary purpose, unless one the exceptions in HPP 10 applies (e.g. emergencies, threat to health or welfare, research or training etc) would generally need the consent of the individual to whom the information relates.	The Audit Office only uses health information for the purpose for which it was collected or a directly related purpose that person would expect. For other uses, the Audit Office seeks consent from the individual to whom the information relates, **unless an exception applies** (e.g., to assist in a stage of an emergency).

Summary of HPP	Audit Office application
Disclosure	
HPP 11 – Limited An organisation that holds health information must only disclose health information for the purpose for which it was collected, or for a directly related purpose that a person would expect. Otherwise, the individual to whom the information relates would generally need to provide their consent, unless one of the exceptions in HPP 11 applies (e.g. in some instances disclosure is allowed in the event of an emergency, serious threat to health or welfare, research or training etc).	The Audit Office will only disclose health information for the purpose for which it was collected, or a directly related purpose that the person would expect. For other disclosures, the Audit Office seeks consent from the individual to whom the information relates, **unless an exception applies** (e.g., to assist in a stage of an emergency).
Identifiers and anonymity	
HPP 12 – Not identified An organisation may only identify people by using unique identifiers if it is reasonably necessary to carry out its functions efficiently.	The Audit Office does not use unique identifiers for health information, as they are not needed to carry out the functions of the Audit Office. Information for audit teams specifies that audit teams should remove unique identifiers from health information that is received.
HPP 13 – Anonymous An organisation must give the person the opportunity of receiving services from anonymously, where this is lawful and practicable.	Not applicable. The Audit Office does not provide health services to individuals.
Transferrals and linkages	
HPP 14 – Controlled An organisation must only transfer health information about an individual outside New South Wales in accordance with HPP 14.	The Audit Office does not usually transfer health information outside of NSW or to Commonwealth agencies. The Audit Office ensures compliance with HPP14 where such transfers do occur.
HPP 15 – Authorised An organisation must only use health records linkage systems if the person has expressly consented to this information being included (this includes disclosure of an identifier).	The Audit Office does not currently use a health records linkage system and does not anticipate using one in the future. However, if one were to be used, the Audit Office would not use one without people's consent.

Appendix 3: Other applicable laws

This section contains information about the other laws that affect how the Audit Office complies with the IPPs and HPPs.

***Government Sector Audit Act 1983* (GSA Act) and *Local Government Act 1993* (LG Act)**

The Audit Office is required under section 38 of the GSA Act and section 425 of the LG Act to preserve the secrecy of information obtained whilst undertaking audit work. Sections 38(2) of the GSA Act and 425(2) of the LG Act contain exceptions to the requirements of the secrecy provisions, meaning the requirements do not apply to:

- the conduct of any matter necessary for the proper administration of the GSA Act or LG Act
- proceedings for an offence relating to government resources or related money or for the recovery of such resources or money
- disciplinary proceedings brought against a government officer or accountable authority for a GSF agency, or
- a report or communication authorised or required to be made by or under the GSA Act or LG Act
- a report or communication that the Treasurer authorises the Auditor-General to make to a person for the purposes of a due diligence or similar process relating to the sale, lease or disposal of any government undertaking (or following such a sale, lease or disposal) or
- a communication that, in the opinion of the Auditor-General, auditor or authorised person, is reasonably necessary for the purpose of exercising a function under the Public Interest Disclosures Act 2022.

Government Information (Public Access) Act 2009* (GIPA Act) and *Government Information (Public Access) Regulation 2018

The object in the GIPA Act is to maintain and advance a system of responsible and representative democratic government that is open, accountable, fair and effective by providing access to government information.

The GIPA Act provides a mechanism to access personal information or other information. An application can be made to the Audit Office to access information that the Audit Office holds. Sometimes, this information may include personal and/or health information. The Audit Office must release information unless there is an overriding public interest against doing so.

The GIPA Act lists a number of considerations which can be taken into account when deciding not to release information to the public. These considerations include whether the disclosure would:

- reveal an individual's personal information
- contravene IPPs under the PPIP Act or the HPPs under the HRIP Act.

In addition, the GIPA Act contains specific provisions relating to information collected or created during the audit process, establishing a presumption that there is an overriding public interest against disclosing information 'related to' the investigative, audit and reporting functions of the Audit Office. In practice, this means that information (including personal or health information) that the Audit Office has collected or created during its investigating, auditing or reporting functions will generally not be disclosed by the Audit Office in response to a GIPA request.

***Independent Commission Against Corruption Act 1988* (ICAC Act)**

The Audit Office has an obligation under section 11 of the ICAC Act to report suspected corrupt conduct to the ICAC. In fulfilling this obligation, the Audit Office may be required to disclose personal information collected during an audit. This obligation to report overrides other secrecy duties or restrictions on disclosure.

***Law Enforcement Conduct Commission Act 2016* (LECC Act)**

The Auditor-General has a duty to report to the Law Enforcement Conduct Commission any matters suspected on reasonable grounds that concern or may concern 'officer misconduct' or 'serious maladministration' under section 33 of the LECC Act. This obligation to report overrides other secrecy duties or restrictions on disclosure.

Public Interest Disclosures Act 2022

Refer to section 6.3 of this Plan.

State Records Act 1998* and *State Records Regulation 2024

The *State Records Act 1998* and Regulation set requirements for public sector agencies relating to the creation, management and protection of records.

Key records management provisions of the Act require public offices to:

- make and keep records that fully and accurately document their business activities
- establish and maintain a records management program in conformity with standards and codes of best practice approved by State Records NSW
- ensure that records, information and data are stored in conditions appropriate to their format and preservation requirements
- ensure that equipment- and technology-dependent records are accessible for as long as they required.

Other key parts of the *State Records Act 1998* include provisions governing the disposal of records, a statutory basis for a right of public access to records more than 20 years old, and the transfer of records required as State archives to the custody and control of Museums of History NSW.

Ombudsman Act 1974

The *Ombudsman Act 1974* defines the functions of the NSW Ombudsman, including complaints handling and oversight of NSW government agencies.

The Audit Office and NSW Ombudsman have entered into a Memorandum of Understanding under section 42 and 43 of the *Ombudsman Act 1974* relating to information sharing and complaint sharing.

The Audit Office may, and in some cases must, disclose information to the NSW Ombudsman to enable the Ombudsman's preliminary inquiries or investigations.

***Privacy Act 1988* (Cth) and *Privacy (Tax File Number) Rule 2015* (Cth)**

The *Privacy Act 1988* (Cth) (the Privacy Act) establishes a Commonwealth Notifiable Data Breaches (NDB) scheme.

Any agency that collects tax file numbers (TFNs) has obligations under the Commonwealth NDB scheme when a data breach occurs involving a TFN.

The Privacy (Tax File Number) Rule 2015 (TFN Rule) issued under section 17 of the Privacy Act regulates the collection, storage, use, disclosure, security and disposal of individuals' TFN information. The TFN Rule requires any organisation holding TFNs to protect the information by implementing reasonable security safeguards in the circumstances.

The obligations under the TFN Rule are in addition to responsibilities under other laws, such as the PPIP Act.

Our vision

Our insights inform and challenge government to improve outcomes for citizens.

Our purpose

To help Parliament hold government accountable for its use of public resources.

Audit Office of New South Wales
Level 19, Darling Park Tower 2
201 Sussex Street, Sydney NSW 2000 Australia
t +61 2 9275 7100
mail@audit.nsw.gov.au
Office hours 8.30 am–5 pm

audit.nsw.gov.au