information and privacy commission
new south wales

Seeking a Public Interest Direction or Code of Practice for a linked data asset

May 2023

Contents

1. Purpose and background 4
2. Is a PID or Code required for the project? 5
3. Which instrument should an agency choose? 5
4. Designing a linked data asset and instrument 6
5. Creating a PID or Code 9
6. What safeguards and privacy protections are being implemented? 11
7. Resources 14
8. Appendices 16

Seeking a Public Interest Direction or Code of Practice for a linked data asset

NSW public sector agencies collect and hold the personal and health information (data) of individuals as part of their functions to provide services to the public. This data can be a rich source of information for the development of new programs and services, making improvements to the delivery of government services and undertaking research which benefits the public.

The creation of a linked data asset enables the extraction of high-value data for more accurate analysis and greater insights to inform decision making and transforms routinely collected data into a resource for research and evaluation.

It is vital that the creation of these assets is undertaken in a way that protects the privacy of the individuals whose information is being shared. The *Privacy and Personal Information Protection Act 1998* (PPIP Act) and *Health Records and Information Privacy Act 2002* (HRIP Act) provide for the use or disclosure of personal and health information for research purposes[1]. In some instances these exemptions may not apply in relation to a proposed linked data asset project and the relevant agency may elect to seek a modification of the Information Protection Principles (IPPs) or Health Privacy Principles (HPPs) to enable the project to be progressed.

This guidance provides agencies with information on the process for seeking a public interest direction or code of practice to authorise the use of personal or health information for the purpose of creating a linked data asset.

This guidance is issued by the Privacy Commissioner under subsections 36(2)(d) and (g) of the PPIP Act and section 58(e) of the HRIP Act. The Commissioner is to provide assistance to public sector agencies in adopting and complying with the IPPs and HPPs and to provide advice on matters relating to the protection of personal and health information and the privacy of individuals.

The Privacy Commissioner acknowledges the expertise and assistance of the NSW Data Analytics Centre in the development of this guidance.

Samantha Gavel

Privacy Commissioner

Information and Privacy Commission NSW

May 2023

[1] Section 27B of the PPIP Act and HPPs 10 and 11 under the HRIP Act.

1. Purpose and background

This guidance is intended to assist NSW public sector agencies to initiate and prepare a Public Interest Direction (PID) or Code of Practice (Code) to enable the creation of linked data assets.

Linked Data Assets

Data linkage is a method of bringing personal and health information (data) from different sources together to create a new, richer dataset.

A de-identified linked data asset is created by merging records from multiple data sources into a single dataset. During this process personal information such as name, address and date of birth is used to link records from each source together. These details are removed once the linkage is completed.

An enduring linked data asset is one that requires on-going linkage of data and regular up-dating of new linked data.

NSW Privacy Legislation

The *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act) govern the way that NSW public sector agencies deal with personal and health information.

The Information Protection Principles (IPPs) and Health Privacy Principles (HPPs) set out what NSW public sector agencies must do when they handle personal or health information. The IPPs and HPPs detail how personal and health information must be collected, stored, used and disclosed, as well as the rights of individuals to access and amend their personal or health information.

Codes of Practice

Codes are statutory instruments that modify the application of the IPPs and HPPs. Codes can be made under either the PPIP Act or the HRIP Act.

A Code can make changes to:

- an IPP or HPP
- the provisions of the PPIP Act that deal with public registers, or
- how an IPP or HPP will apply in a particular situation.

Codes must not impose stricter obligations than the IPPs or HPPs and they should not be seen as a tool for blanket exemptions to the principles.

The IPC has published Guidance on the preparation and assessment of Privacy Codes of Practice under the PPIP Act and HRIP Act, which is designed to help public sector agencies to understand their obligations when seeking a Code under the PPIP Act or the HRIP Act.

A list of Privacy Codes that have been approved and gazetted is also available for reference on the IPC's website.

Public Interest Directions

PIDs are another type of statutory instrument that can be made to modify the application of the IPPs and HPPs under the PPIP Act or HRIP Act.

A PID modifies the application of the IPPs/HPPs or a Code of Practice to particular projects or activities of one or more public sector agencies, generally for a limited time period. A PID cannot permit conduct that would be otherwise be unlawful and does not override other laws, contracts or agreements which already affect an agency.

If a longer-term exemption or modification is required for a project or activity, a Code or legislative amendment may be required.

The IPC's Guide to Seeking a Public Interest Direction under NSW privacy laws outlines the purpose of a PID and provides direction on what needs to be included when seeking a PID.

A list of Public Interest Directions currently in operation and a list of superseded directions is available on the IPC website and provides a useful selection of operational PID examples for review.

2. Is a PID or Code required for the project?

Generally, if an agency intends to collect, use or disclose personal or health information in ways that do not comply with either the IPPs or the HPPs, they will likely require either a legislative amendment or a PID or Code to do so, unless there is an existing law that permits the agency to use information in this way.

There are a range of exemptions under the privacy legislation that may apply to authorise the collection, use or disclosure required for your project.

For example, if your project has been approved by a Human Research Ethics Committee then you can likely rely on the research exemptions in the PPIP Act (s. 27B) and the HRIP Act (Sch. 1, clauses 10(1)(f) and 11(1)(f)). If you can rely on the research exemptions, you will not need a PID or Code. The Privacy Commissioner has published Statutory Guidelines on Research under both the PPIP Act and HRIP Act.[2]

You should seek legal advice first to determine whether a PID or Code is required.

Should your project require significant modification of, or exemption from, the IPPs or HPPs, a legislative amendment is usually the preferred option for seeking these changes.

You should also consider whether there are technology solutions that could be applied to your project that would enable it to be conducted in a more privacy protective way. The use of privacy enhancing technologies may assist your agency to undertake your project in a privacy protective manner and may enable the project to proceed without the need for a PID or Code.[3]

3. Which instrument should an agency choose?

Do I need a PID or a Privacy Code?

The agency needs to determine whether a PID or a Code is the most appropriate instrument for your project. As a general rule, a PID is suitable for projects or activities that are temporary in nature or limited in scope.

A Code is more appropriate for projects or activities that are permanent or more enduring in nature, or broad in their proposed scope of activities.

Does my linked data asset require the sharing of personal information or health information or both?

You should determine whether you need to use or disclose personal or health information, or both, in order to create your linked data asset:

- If you only need to use or disclose personal information, then you may need a PID or Privacy Code under the PPIP Act.
- If you only need to use or disclose health information, then you may need a Health PID or a Health Privacy Code under the HRIP Act.

---

[2] Statutory Guidelines on Research – Section 27B

Use or disclosure of health information for research purposes

[3] For further information on privacy enhancing technologies see the PET Symposium and guidance released by the UK Information Commissioner's Office.

- If you need to use or disclose both personal and health information, you may need a PID or Privacy Code under the PPIP Act and a second instrument drafted in equivalent terms under the HRIP Act (i.e., a PID and a Health PID or a Privacy Code and a Health Privacy Code).

If you are not sure, seek legal advice.

Instrument	When to use	
	Type of information	**Type of project**
PID	Personal information	• Ad hoc data linkages • One off data linkages (i.e., where data is only linked once and is not updated) • Trials or pilot programs • Transitional arrangements • Urgent projects (with a Privacy Code possibly to follow)
Privacy Code	Personal information	• Creation of enduring linked data assets that require updating over time
Health PID	Health information	• Ad hoc data linkages • One-off data linkages (i.e., where data is only linked once and is not updated) • Trials or pilot programs • Transitional arrangements • Urgent projects (with a Health Privacy Code possibly to follow)
Health Privacy Code	Health information	• Creation of enduring linked data assets that require updating over time

4. Designing a linked data asset and instrument

Project objectives

Before the agency commences consultation with the Privacy Commissioner, it should:

- Clearly identify the purpose and scope of the project
- Identify what data is required for the project and where it can be sourced
- Identify any other agencies or third-party organisations that will participate in the project.

The agency should use this initial scoping activity to develop the structure for a supporting business case on the PID or Code, which will be submitted as part of the application/consultation (See section 5 below).

Designing your technical solution

In preparation for designing a technical solution, the project team will need to document the proposed information flows, showing where data is collected, used and disclosed and by which agency. Documenting the proposed information flow will identify which other agencies will be part of the data sharing process and who needs to be consulted during the development of the project.

A technical solution that includes safeguards and mitigates risk of privacy breaches is critical.

Agencies proposing to develop linked data assets that involve both de-identification and data matching processes should also consider relevant published guidelines that relate to these processes.

The IPC has published general guidance on the de-identification of information which may be useful in helping an agency develop de-identification processes.

The Office of the Australian Information Commissioner (OAIC) and Data61 have developed a de-identification decision making framework that can assist agencies that handle personal information and need to share or release it in a de-identified format. The OAIC has also published detailed guidance on data matching in Australian Government administration. While these guidelines relate to obligations on Australian Government agencies subject to the *Privacy Act 1988* (Cth), they may also assist NSW government agencies to develop robust de-identification processes.

Use of intermediaries

A PID or Code may provide for the use of an intermediary, such as a Data Linkage Centre or a Data Analytics Entity. Your privacy impact assessment (see below) needs to address the use of any such entities. Modification of the IPPs or HPPs may be needed to so that personal or health information can be disclosed to them, and used by them, for the purpose of the project. See section 5 for further information on data linkage centres and data analytics entities.

Role and responsibilities

Defining roles and responsibilities within the project team ensures everyone knows the degree of involvement that is required from them to achieve the project objectives. Establishing clear roles and responsibilities also assists in developing project governance and communications.

The agency should clearly define:

- Who is responsible for the project?
- Who will be managing the technical aspects of the project and what qualifications they have?
- Other parties (e.g., contracted service providers) and their roles, including the types of information they will be collecting and how they will use or disclose that information.

Conduct or obtain a Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an analysis of a project to identify:

- the impact of the project on the privacy of the individuals whose personal or health information is to be collected, used or disclosed, and
- whether the information handling proposed by a project has the potential to breach the IPPs or HPPs.

A PIA should make recommendations concerning mitigation strategies to be adopted to address the identified privacy risks.

As part of the PIA process, you should ensure that you have documented the proposed information flows, showing where data is collected, used and disclosed by each participating agency. Documenting the proposed information flow will identify which other agencies will be part of the data sharing process and how modifications or exemptions should be drafted to ensure that all participating agencies are covered. The information flow should include the technical solution utilised for the linkage.

The PIA should include an assessment of each type of information handling (eg, collection, use, disclosure, security, etc) by each participating agency against the applicable IPP or HPP.

For a data linkage project, the main principles that will likely require modification or exemption are those that generally prohibit collection from third parties, use and disclosure. However, each project is different, and a comprehensive PIA should consider whether the project complies with each of the IPPs or HPPS and consider the potential privacy impacts and risk to individuals in a holistic manner.

PIAs may be done internally or outsourced to an independent privacy consultant.

The IPC does not require agencies to use a specific format when drafting a PIA. Should you require further information on how to develop a PIA, the IPC's A guide to Privacy Impact Assessments includes a suggested outline of the form and content of a PIA.

Following completion, you should consider whether the PIA should be made publicly available to inform members of the public about the project. This builds trust, as it shows that the agency has carefully considered privacy and put in place controls to protect personal and/or health information.

In some circumstances an agency may choose to publish a redacted version of the PIA. Examples of circumstances where it may be necessary to redact the PIA may include where publication of the full PIA could:

- reveal commercial in confidence information relating to third party participants
- reveal information about the information management or cyber security arrangements of the agency that could result in risks to security.

Establishing a business case – make a convincing case

In assessing the need for a PID or a Privacy Code, the Privacy Commissioner needs to clearly understand the agency's case for the public interest in making the instrument. The agency will need to clearly explain the purpose of the project and demonstrate how the public interest in making the instrument will outweigh the public interest in complying with the IPPs/HPPs.

The business case should detail:

- the public interest case for making the instrument
- any privacy mitigations developed to address the recommendations of the privacy impact assessment for the project
- where relevant, the data matching protocol to be utilised, and
- proposed data governance arrangements including data sharing agreements and data access, security and audit arrangements.

Draft your instrument

A PID or Code is a legal instrument that alters the legal obligations an agency is required to comply with under the privacy legislation. It is therefore strongly recommended that you seek legal assistance to draft the PID or Code.

The IPC has published a checklist to assist agencies with the process of preparing a PID or Code. It includes a number of prompts and questions for issues to consider during this process and an indicative outline of the format and content of an instrument.

5. Creating a PID or Code

Who makes the instrument and who must be consulted?

There are no prescribed forms to use when seeking a PID or Code. However, the legislation specifies who makes the instrument, and who must be consulted. This depends on what type of instrument is being sought:

Instrument	Process	
	Who makes the instrument	**Who must be consulted**
PID	Privacy Commissioner	Approval must be obtained by the NSW Privacy Commissioner from the Attorney General and Minister for Customer Service and Digital Government[4]
Privacy Code	Attorney General and Minister for Customer Service and Digital Government	NSW Privacy Commissioner and other appropriate stakeholders must be consulted[5]
Health PID	Privacy Commissioner	Approval must be obtained by the NSW Privacy Commissioner from the Minister for Health Attorney General must be consulted by the NSW Privacy Commissioner [6]
Health Privacy Code	Minister for Health	NSW Privacy Commissioner, Attorney General and other appropriate stakeholders must be consulted[7]

Stakeholder consultation

Stakeholder consultation is an important part of the process and the time taken to consult with stakeholders needs to be considered in the overall project time frames. As a minimum, the project team will need to consult with the NSW Department of Communities and Justice (DCJ) and the Department of Customer Service, as the Attorney General and Minister for Customer Service and Digital Government jointly administer the PPIP Act. If you propose to share health information, you will need to consult the Ministry of Health.

It can be helpful to create a Stakeholder Consultation Plan at the beginning of the project, identifying who needs to be consulted, by when and how they are to be consulted. Project leads may need to seek legal advice prior to consulting with the IPC.

Approval process - timeframes and sequencing

The timeframe for obtaining a PID or Code varies depending on the urgency of the circumstances and the complexity of the matter, including the number of agencies involved in the data sharing, the public interest and whether any intermediary is used to create the data linkages.

[4] Section 41 of the PPIP Act

[5] Section 31 of the PPIP Act

[6] Section 62 of the HRIP Act

[7] Section 40 of the HRIP Act

Appendices 2 and 3 of this guidance set out the various steps and estimated time frames involved in obtaining PIDs and Codes.

Memorandums of Understandings/Information Sharing Agreements

Where project participants are disclosing personal or health information it is recommended this process be documented in a memorandum of understanding (MOU) or data sharing agreement.

An MOU or data sharing agreement:

- sets out the roles and responsibilities of all parties
- sets out the purposes for which data may be used or disclosed
- establishes what happens to the data at each stage.

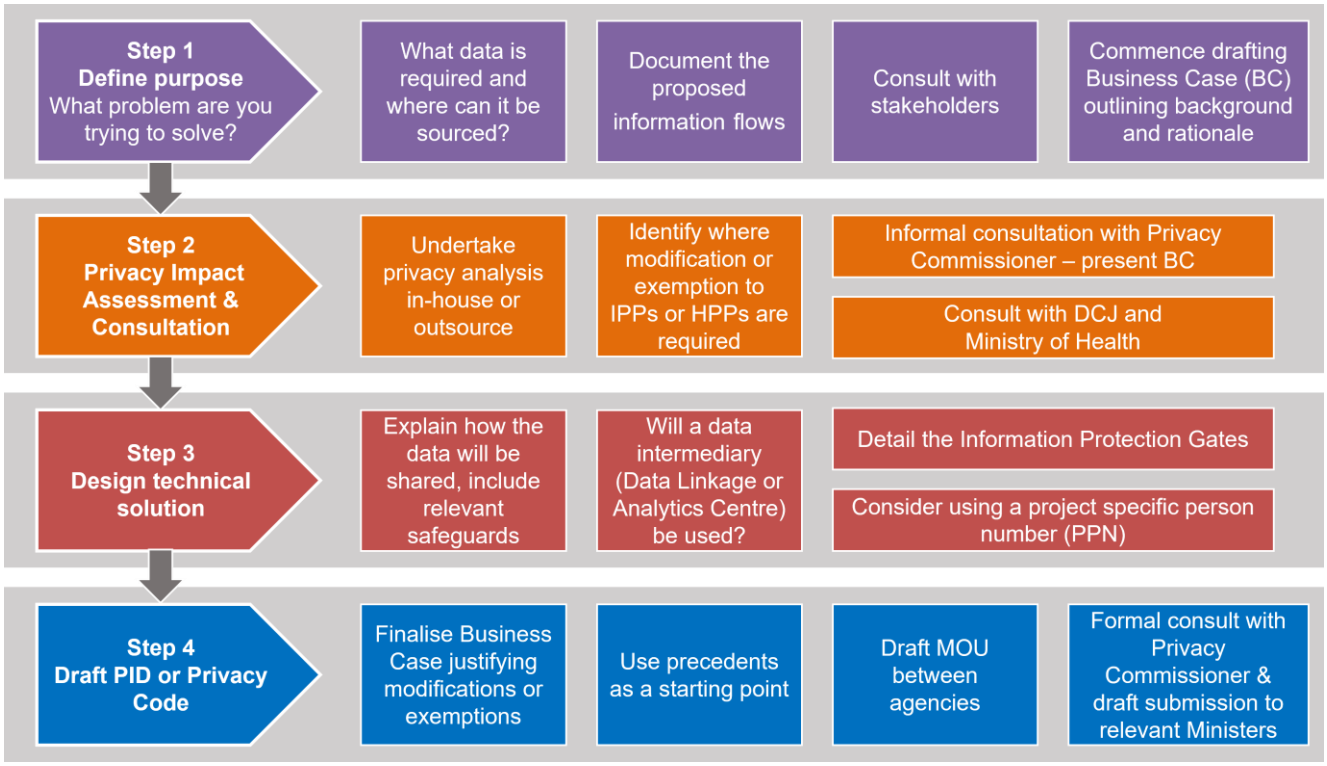
There is no set format for an MOU or data sharing agreement; it can take a variety of forms, depending on the scale and complexity of the data sharing. Since an MOU or data sharing agreement is a set of common rules that binds all the parties involved, it should be drafted it in clear, concise language that is easy to understand.

Specifically, it should include:

- the name and contact details of the parties to the agreement and their specific roles and responsibilities in the project
- a description of the project, its benefits, the expected outcome(s) of the project and any outputs that will be produced
- the specific data that is being shared
- whether any personal or health information is being shared and the legal authority for sharing this data
- the purpose for sharing the data
- an acknowledgement that the data is being shared in compliance with all relevant legislation
- the name and contact details of the data owner and/or data custodian within all parties to the agreement
- how the data will be shared and the measures to be implemented to ensure the information is shared securely
- how the data will be stored by the recipient
- the specific persons or roles within each party that are permitted to access and use the personal information. This could include a minimum level of seniority or security clearance.
- details of whether individuals who will be handling the data are required to undertake any training or meet certain requirements before being permitted to access and use the data
- the purposes for which the personal information can and cannot be used.
- how consent arrangements have been addressed - note that consent will only be applicable in some circumstances
- whether a PIA has been undertaken and any privacy risks identified as a result of the PIA. Also include information on whether a security risk assessment has been completed and the outcomes
- whether there are constraints on the further release of the data
- how any data corrections will be handled
- the details of ongoing audit or monitoring arrangements

- the details of how data will be disposed or returned at the end of the agreement
- the archiving responsibilities of each party in relation to the State Records Act, if applicable
- any other obligations resulting from enabling legislation of either party
- the date, time and duration of the agreement.

Steps in seeking a Public Interest Direction (PID) or Code of Practice



6. What safeguards and privacy protections are being implemented?

Stringent measures and controls need to be built into the Project to protect the privacy of individuals and to mitigate potential privacy breaches. Privacy training should always form a key measure put in place by agencies to protect the privacy of individuals, particularly before any system is developed that will provide employees or contracted service providers with access to personal or health information.

Agencies should consider assessing the project elements based on the Five Safes framework, an internationally recognised approach to considering strategic, privacy, security, ethical and operational risks as part of a holistic assessment of the risks associated with data sharing or release.[8]

[8] For further information on the Five Safes framework https://www.aihw.gov.au/about-our-data/data-governance/the-five-safes-framework

Element	Meaning	Self-Assessment of your project and how these elements will be managed
Safe people	Researchers have the knowledge, skills and incentives to act in accordance with required standards of behaviour.	• Are the users appropriately authorised to access and use the data? • Only limited and authorised personnel within Participating Agencies and Public Sector Agencies, and with appropriate delegation, will have the authority to collect, use and disclose personal and health information related to the project. All entities and persons that that may be provided with information will be subject to privacy and confidentiality obligations to protect it from unauthorised use and disclosure. • Authority to collect, use and disclose
Safe projects	Use of the data is legal, ethical and the project is expected to deliver public benefit	• Is the data to be used for an appropriate purpose, such as a valid research aim, a public benefit and won't be used for compliance or regulatory purposes?
Safe data	Data has been treated appropriately to minimise the potential for identification of individuals or organisations.	• Is there a disclosure risk in the data itself? • Allocate a project specific person number (PPN), unique to the Project and the individual.[9] • Separate Identifier Information and Service Usage Data within the Data Linkage Centre.[10] • Apply appropriate Information Protection Gates
Safe settings	There are practical controls on the way the data is accessed – both from a technology perspective and considering the physical environment.	• Does the access facility prevent unauthorised use? • Consider Tiers of data to manage the flows and access to data. • Use secure systems and processes, including the use of secure file transfer protocol to transfer data to the Data Analytics Entity.
Safe output	This is the final check on the information before it is made public, and the findings of the project are released.	• Are the statistical results non-disclosive?

[9] The PPN should not follow a pattern such that it could be deciphered to identify a particular individual or class of individuals. The PPN should not be generated from any aspect of the Personal or Health Information that it relates to, and therefore it is not associated with any Identifier Information.

[10] This separation creates a safeguard against identifying individuals and their recorded information outside the Participating Agency that holds the original record.

Privacy protections and controls

Some key privacy controls that agencies should consider adopting include:

- allocating a PPN to all individuals. For privacy purposes, each PPN is unique to the Project and the individual and does not follow a pattern such that it could be deciphered to identify a particular individual or class of individuals. Furthermore, the PPN is not generated from any aspect of the Personal Information that it relates to, and therefore it is not associated with any Identifier Information
- the use of secure systems and processes, including the use of a secure file transfer protocol and encryption to transfer data to other parties
- ensuring that only limited and authorised persons can access personal or health information in connection with the project, which must be accessed with secure access controls
- build in systems which will allow for regular reporting on use of the data asset, this could be systems ranging from the logging of file access to individual keystrokes and data viewing
- the implementation of a governance framework for the project, which will include a framework for the protection of personal and health information and a transparent process to request, handle and secure datasets.

Data Linkage Centre

A data linkage centre provides a service or function to undertake data linkage for the project.

The Centre for Health Record Linkage (CHeReL) is one example of a data linkage centre. The CHeReL links multiple sources of data and maintains a record linkage system that protects privacy through their compliance with best practice principles which includes the separation of the linkage of personally identifying information from the analysis of de-identified linked health records. By providing a mechanism for researchers to access de-identified linked data, the CHeReL enables ethically approved research in the public interest to be carried out without consent, minimising bias and allowing researchers to access data on whole populations.

Whether your agency chooses to contract with a data linkage centre will depend on the specific context of your data linkage project. Some factors for consideration in making this decision may include:

- The type and sensitivity of the information being disclosed
- The size and profile of the cohort being researched
- The number of datasets being linked
- Whether your agency possesses the technical expertise to undertake the linkage.

Data Analytics Entity

The technical solution for the creation of a linked data asset could involve the engagement of a data analytics entity such as the NSW Data Analytics Centre (DAC), or another entity that is under a contractual obligation to comply with the privacy legislation. The entity would need to be, or be engaged by, a public sector agency and be compliant with the NSW Government Digital Information Security Policy.

The NSW Data Analytics Centre (DAC) provides a central data platform that facilitates data sharing and collaboration, combating operational silos and focusing on state-wide outcomes. Government-wide data-sharing and collaboration is encouraged and enabled through the DAC's provision of:

- analytics and data science approaches to realise the potential of data and improve customer outcomes;
- building a strong data culture to promote the release, sharing and use of data;

- secure and strongly governed data infrastructure, data visualisation capabilities and provision of self-service analytics.

Reporting and auditing

PIDs and Codes usually contain provisions on reporting and auditing.

A PID or Code should include provisions that establish the mechanisms which will be implemented by the agency to give assurance that the personal or health information disclosed as part of the project has been handled in accordance with terms of the PID or Code. This could include the ability to audit unit level access to personal or health information, or the requirement to conduct annual external audits.

For example, a PID or Code may require an agency to report annually to the Privacy Commissioner on matters such as:

- Confirmation regarding the correctness of any and all uses and disclosures in connection with the project;
- Details of any complaints received from the public regarding the Project; and
- Any circumstances where there have been any data breaches involving personal or health Information or where such breaches could have arisen[11].

The Project Team (or its authorised representative) will audit and assess whether there are sufficient security systems and processes in place to protect personal and health information that is collected, used and disclosed as part of the project and submit the results of this audit with the annual report to the Privacy Commissioner.

You may wish to review previously approved PIDs and Codes published on the IPC website for examples of how these requirements have been adopted.

7. Resources

IPC resources

- Information Protection Principles for agencies
- Health Privacy Principles for agencies
- Privacy by design
- Statutory Guidelines on Research – section 27B
- Use or disclosure of health information for research purposes
- Guide to Privacy Impact Assessments
- Seeking a public interest direction under NSW privacy law
- Guide on the preparation and assessment of Privacy Codes of Practice under the PPIP Act and HRIP Act
- Checklist: Preparing a public interest direction of code of practice
- De-identification of personal information
- Data Sharing and Privacy

[11] The commencement of the Mandatory Notification of Data Breach Scheme on 28 November 2023 will replace the need for the inclusion of provisions concerning data breach reporting.

Other resources

- Office of the Australian Information Commissioner and Data61: de-identification decision making framework
- Office of the Australian Information Commissioner: guidelines on data matching in Australian Government administration
- Australian Institute of Health and Welfare: Five Safes Framework

NOTE: The information in this Guide is to be used as a guide only. Legal advice should be sought in relation to individual circumstances

8. Appendices

Appendix 1 – Sample business case

Project Details

Name of project	
Name of lead agency	
Date	
Executive Sponsor/s	Name: Agency: Email:
Project Manager	Name: Agency: Email:
Privacy Officer	Name: Agency: Email:
Data Custodians	*Insert all data custodians by agency, business unit and contact person*
Data Recipient/s	*Include any agency, business unit or person who will receive the data as a result of the data sharing.*
Is a data intermediary being proposed? If so, please provide details.	*Include details about any proposed data intermediary such as a Data Linkage Centre or Data Analytics Centre*
What is the anticipated timeframe for the project?	*Please note that PIDs authorise a temporary departure from the IPPs and/or HPPs. This includes for an urgent data or cyber breach that requires remediation, a pilot or one-off project or as an interim arrangement.* *Where an enduring data asset is being created as a part of your project, that will be updated over time, you should consider seeking a Code rather than a PID.*
Are legislative amendments required (e.g., in addition to the PID/Code or subsequent to the PID/Code)	

Has a Privacy Impact Assessment (PIA) been completed and attached?	*A PIA can be undertaken internally within a NSW Government agency or outsourced to an independent privacy consultant. Please include a brief description here.*
Stakeholder consultation	*Include or attach the details of the consultation undertaken in the drafting of the PID or Code*

Project Objectives and the Public Interest

This section needs to include a clear statement of the project purpose and the ways in which the data sharing and linkage will benefit the public. When assessing your proposal for a PID or Code, the Privacy Commissioner needs to understand the public interest of your project and if this public interest outweighs the public interest in the relevant agencies complying with their usual privacy obligations.

Before proceeding with a proposal to obtain a PID or Code, agencies need to consider if there are other mechanisms available that can be employed to achieve the purpose of the project. Agencies should consider and exhaust all other options within the NSW privacy legislation and their enabling legislation before opting to seek a PID or Code. It is important to note that PIDs and Codes will be publicly available through the IPC website once they have been finalised, therefore careful consideration should be given to what information is appropriate for public release.

Issues to consider:

What are the overall project objectives and what outcomes will the data sharing project achieve?

Other elements to include:

- The scope and extent of the project
- Any links with other programs or projects with the agencies involved or across NSW Government more broadly

Roles and Responsibilities

This section states who is involved in the project and clearly describes the roles and responsibilities of each responsible person and agency.

Issues to consider:

- Who is responsible for the project?
- Who will be managing the technical aspects of the project and what qualifications they have?
- Other parties (e.g., contracted service providers) and their roles, including the types of information they will be collecting and how they will use or disclose that information.
- A RACI table can be used to identify who is responsible, accountable, consulted and informed if helpful.[12]

[12] For further information on using RACI https://project-management.com/understanding-responsibility-assignment-matrix-raci-matrix/

Stakeholder consultation

This section should provide information on the consultation that has been undertaken in developing the PID or Code.

Issues to consider:

- Who has been consulted on this project, what has been the consultation methodology, scope and extent?
- Have other agencies been consulted on the proposed PID or Code?
- What are the views of stakeholders and to what extent are they supportive of the need for a PID or Code?
- Were stakeholders able to identify alternative mechanisms to achieve the project objectives rather than requiring a PID or Code?
- Were agency stakeholders able to identify linkages and benefits to other projects they are involved in, or have in the pipeline?
- Has citizen input been gathered, and if so, what are the views of citizens?

Appendix 2 - Indicative timeframes and sequencing when making PIDs and Health PIDs

The following timeframes are indicated as a guide only. Please note that some tasks may be undertaken concurrently to shorten the overall timeframe.

This table is intended to be a guide to help you work through the various tasks required to obtain a PID or a Health PID.

Task	Notes	Possible timeframe
Define the purpose and scope of the project	Identify the purpose of the project and what its scope is. Identify and articulate the public interest in the project going ahead. The agency should use this initial scoping activity to develop the structure for a supporting business case on the PID, which will be submitted as part of the application.	Up to 2 weeks
Document the proposed information flows	Documenting the proposed information flow will identify which other agencies will be part of the data sharing process. These agencies should be consulted.	Up to 4 weeks
Undertake an initial privacy analysis	Consider any statutory information sharing provisions that may apply – in that case, it may not be necessary to obtain a PID. NOTE that a PID is not capable of overcoming any secrecy provision that restricts the sharing of information in particular circumstances. Seek legal advice if you are unsure.	Up to 4 weeks
Design a technical solution	Explain how the data will be shared, including in relation to what technology platforms and processes will be used for collection and disclosure of personal information. The details of enabling IT and communications infrastructure will need to be incorporated in the PID application, and the subject of assessment in related Privacy Impact Assessments. Consideration of technical solutions may also require the completion of a Security Risk Assessment (see below). These steps will inform the PID when you draft it.	Up to 4 weeks
Informal consultation with IPC	Initiate contact with the Privacy Commissioner. Provide a short business case and outline the background and rationale for the request.	Up to 2 weeks
Informal consultation with DCJ and DCS (and Ministry of Health if applicable)	Initiate contact with DCJ and DCS and indicate that you are seeking a PID. Provide any information or documents requested. Consult the Ministry of Health if health information is involved.	Up to 4 weeks
Undertake or obtain a privacy impact assessment	This will provide more precise information about what modifications or exemptions are necessary with respect to each aspect of the information flow. It should also identify what safeguards or mitigations should be implemented.	Up to 4 weeks
Undertake or obtain a security risk assessment for relevant technology platforms	For activities that require specific technology platforms to enable collection, disclosure or retention of personal information, the agency may need to undertake a specific security risk assessment of the relevant technology solution. While this assessment may not need to be completed at the time the PID application is completed, the agency should be	Up to a month

Task	Notes	Possible timeframe
	in a position to provide the Privacy Commissioner with advice on the proposed assessment	
Draft the PID	Use precedents as a starting point. Include project objectives as these will be helpful if a question about interpretation arises. Describing the information flows involved in the project. A high-level diagram of dataflows may be useful to support the text. Consult with the data analytics team which is managing the dataflows to ensure the draft captures their activities. The PID will be published on the IPC website so ensure that the information included is suitable for publication. Ensure the term of the PID is adequate to allow for unforeseen delays etc in the process. Share the draft as widely as possible to obtain input. Obtain legal advice as necessary.	Up to 4 weeks
Provide the draft PID to the NSW Privacy Commissioner	Provide the PID in draft to the Privacy Commissioner and offer to meet to discuss it. Make any amendments to the draft following consultation with the Privacy Commissioner.	Up to 2 weeks
Draft MOU between agencies which are collecting, using, disclosing data.	Consult with the other agencies participating in the data exchange on the terms of the MOU. This document will be important for any audit required by the Privacy Commissioner.	Up to 4 weeks
Formally submit the request for a PID to Privacy Commissioner	Provide the Privacy Commissioner with the finalised draft PID and any supporting documents including the business case and PIA	4 weeks
Privacy Commissioner seeks Minister's approval	Before making a PID the Privacy Commissioner must seek the approval of the Minister.	2-4 weeks
Making and publication	If Privacy Commissioner approves the PID application, the IPC will publish the signed Direction and advise the agency.	1 week

Appendix 3 - Indicative timeframes and sequencing when making Privacy Codes and Health Privacy Codes

This table is intended to be a guide to help you work through the various tasks required to obtain a Privacy Code or a Health Privacy Code.

Task	Notes	Possible timeframe
Define the purpose and scope of the project	Identify the purpose and scope of the project.	Up to 2 weeks
Document the proposed information flows	Documenting the proposed information flow will identify which other agencies will be part of the data sharing process. These agencies should be consulted.	Up to 4 weeks
Undertake an initial privacy analysis	Consider any statutory information sharing provisions that may apply – in that case, it may not be necessary to obtain a Code. NOTE that a Code is not capable of overcoming any secrecy provision that restricts the sharing of information in particular circumstances. Obtain legal advice as necessary.	Up to 4 weeks
Design a technical solution	Explain how the data will be shared, including in relation to what technology platforms and processes will be used for collection and disclosure of personal information. The details of enabling IT and communications infrastructure will need to be incorporated in the Code application, and the subject of assessment in related Privacy Impact Assessments. Consideration of technical solutions may also require the completion of a Security Risk Assessment (see below). These steps will inform the Code when you draft it.	Up to 4 weeks
Informal consultation with DCJ and DCS (and Health if applicable)	Initiate contact with DCJ and DCS and indicate that you are seeking a Code. Provide any information or documents requested, Consult the Ministry of Health if health information is involved.	Up to 2 weeks
Identify any other relevant stakeholders and consult them	Share the draft as widely as possible to obtain input. Consult with data analytics teams which are managing the dataflows to ensure the draft captures their activities. Obtain letters of endorsement if appropriate to include when briefing the Privacy Commissioner.	Up to 2 weeks
Undertake or obtain a privacy impact assessment	This will provide more precise information about what modifications or exemptions are necessary with respect to each aspect of the information flow. It should also identify what safeguards or mitigations should be implemented.	Up to 4 weeks
Undertake or obtain a security risk assessment for relevant technology platforms	For activities that require specific technology platforms to enable collection, disclosure or retention of personal information, the agency may need to undertake a specific security risk assessment of the relevant technology solution. While this assessment may not need to be	Up to 4 weeks

Task	Notes	Possible timeframe
	completed at the time the PID application is completed, the agency should be in a position to provide the IPC with advice on the proposed assessment.	
Prepare a detailed business case	This should be a detailed justification for the modifications or exemptions you are seeking. You should explain what the problem is and how the project is going to solve it. You should explain why non-compliance with the IPPs or HPPs is warranted in the circumstances.	Up to 2 weeks
Draft the Code	Use precedents as a starting point. Include objectives as these will be helpful if a question about interpretation arises. Describing the information flows involved in the project. A high-level diagram of dataflows may be useful to support the text. Include a review clause.	Up to 4 weeks
Draft MOU between agencies which are collecting, using, disclosing data	Consult with the other agencies participating in the data exchange on the terms of the MOU. This document will be important for any audit required by the IPC.	Up to 4 weeks
Consultation with IPC	Provide a detailed briefing to the NSW Privacy Commissioner including your detailed business case, draft and letters of endorsement from relevant stakeholders. Offer to meet to discuss it. The Privacy Commissioner is likely to adopt the approach that the impact on privacy must be kept to the minimum necessary to allow the data exchange process to occur.	Up to 2 weeks
Make any amendments to the draft Privacy Code in consultation with the Privacy Commissioner	Make any amendments to the draft following consultation with the Privacy Commissioner.	Up to a week
Approval by the Privacy Commissioner	Submit the final draft of the Code to the Privacy Commissioner for approval.	1-2 weeks
Draft submission to relevant Ministers	The submission should indicate that the Privacy Commissioner has been consulted. The relevant agencies can advise on the most efficient way to obtain the input or approval of the Ministers. The Privacy Commissioner may elect to make a submission to the Minister in relation to the Code.	Up to 4 weeks
Code is made	The Code is made by an order of the Minister published in the Gazette. The Code takes affect when the order making the Code is published (unless a later date is specified). A Code will remain in effect until it is revoked by the relevant Minister or superseded by legislation.	Up to 8 Weeks

Document information

Identifier/Title:	Seeking a Public Interest Direction or Code of Practice for a linked data asset
Business Unit:	IPC
Author:	Legal Counsel and Regulatory Advice
Approver:	Privacy Commissioner
Date of Effect:	1 May 2023
Next Review Date:	1 May 2025
EDRMS File Reference:	D22/038624/DJ
Key Words:	Personal information, health information, disclosure, public interest direction, code of practice, exemption