information and privacy commission
new south wales

Data Sharing and Privacy:

a guide for public sector agencies

July 2020

Contents

Data Sharing and Privacy

The sharing of data between public sector agencies and appropriate third parties can support more informed policy making, program management and evaluation, research and service planning. Sharing data safely can facilitate better policy decision-making and more efficient service delivery for citizens and business.

Before a NSW public sector agency shares data they will need to make sure that they comply with the privacy and data protection requirements set out in legislation, as well as any agency-specific data sharing policies. This guidance explains the key considerations that agencies should address before they share data.

The framework within which data sharing is carried out includes key legislation establishing controls on data sharing, as well as providing mechanisms through which data may be shared.

- The *Privacy and Personal Information Protection Act 1998* (PPIP Act) establishes controls and obligations on the disclosure of personal information.
- The *Health Records and Information Privacy Act 2002* (HRIP Act) governs the management of health information held by organisations (public sector agencies or a private sector person) that are health service providers or that collect, hold or use health information. This includes hospitals both public and private, doctors, other health service providers and any other organisations that handle health information. More specifically the Act applies to public sector agencies, private sector organisations that provide a health service or collects, holds or uses health information, and private sector organisations including some businesses that are related to another business, with an annual turnover of more than $3 million that collect, store or use health information
- Public sector agencies are authorised to share data with another public sector agency for specific purposes under the *Data Sharing (Government Sector) Act 2015* (Data Sharing Act).
- Other legislation may contain specific provisions authorising or requiring the sharing of data by an agency with specified bodies or equivalent bodies in another jurisdiction.

Private organisations and other public sector agencies may request data directly from an agency on an ad hoc basis or as part of a formal on-going data sharing arrangement. This guidance includes key considerations that public sector agencies should address regardless of the proposed mechanism used to share data.

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 information protection principles and to provide advice on matters relating to the protection of personal information and the privacy of individuals.

Samantha Gavel

Privacy Commissioner

Information and Privacy Commission NSW

July 2020

1. Who has made the request?

How your agency shares data will vary depending on what data is being requested and who is making that request. For example, you will use a different mechanism to share data if your agency receives a request to share data from another government sector agency compared to a request from a non-government entity such as a research centre or industry peak body.

1.1 Sharing with NSW government agencies

The Data Sharing Act authorises NSW government sector agencies to share data with other NSW government sector agencies for specific purposes as set out in the legislation (see section 2.3 below).

The Act operates to authorise data sharing that might otherwise be prohibited under other legislation. Where the sharing is compliant with the requirements of the Data Sharing Act, the provisions in other legislation prohibiting disclosure of information obtained in connection with the administration of that legislation do not apply.

However, any sharing that occurs under the Data Sharing Act must be done in accordance with the PPIP Act, HRIP Act and any applicable Public Interest Direction or Privacy Code of Practice made under the privacy legislation.

The Act does not authorise data sharing with Australian Government agencies or the agencies of another State or Territory.

1.2 Sharing with entities outside the NSW Government sector

Agencies may also receive a request for data from an entity or organisation outside the NSW Government sector. A request of this type may come from a government agency in another state or territory or from an Australian Government agency. This type of request might also be received from a non-government organisation such as a research institute or other organisation.

When considering a data sharing request from outside the NSW Government sector, you should carefully consider the matters set out in this guidance, comply with the requirements of the PPIP Act or HRIP Act where relevant and apply the data sharing principles to guide your consideration.

2. Deciding to Share Data

It is important that data sharing decisions are made with a thorough understanding of the data involved and what the consequences of sharing that data will be. The following process should be used in order to determine the relevant risks and mitigations when responding to a request to share data.

2.1 Identify the type of data

The first step in responding to a request to share data is identifying what type of data has been requested. The type of data will inform the risks and responsibilities that go along with sharing that data.

The following are general broad categories of data but you should also consider whether there are more specific categories that are appropriate to your agency. Keep in mind that data may belong to more than one of these categories.

- **Government sector data –** this covers any data held or controlled by a government sector agency. Government sector data may be shared to identify issues and solutions regarding Government policy making, program management and service planning and delivery by government sector agencies. Most statistical data useful for analytics would fall into this category.
- **Confidential or commercially-sensitive information** – this is information that falls under a commercial-in-confidence or contractual agreement or is otherwise confidential or commercially-sensitive. The Data Sharing Act states this data can only be shared in a way that complies with the terms of the agreement or contract.
- **Personal information** – means any information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

  Examples of information that would be defined as personal information include:

  - names, addresses and other details about an individual
  - photographs, images, video or audio footage of an individual
  - fingerprints, retina prints, blood or DNA samples.

  The full definition of personal information, including exceptions, can be found in section 4 of the PPIP Act.

  Generally, any sharing of personal information must be done in full compliance with the information protection principles (IPPs) in the PPIP Act, unless one of the exceptions or exemptions under the PPIP Act applies or a Public Interest Direction or Privacy Code of Practice operates to provide an exemption. For more information on the IPPs see the IPC website.
- **Health information** – this is a type of personal information and includes any data that is information or an opinion about:
  - the physical or mental health or a disability (at any time) of an individual
  - an individual's express wishes about the future provision of health services to him or her
  - a health service provided, or to be provided, to an individual
  - other personal information collected to provide, or in providing, a health service

- other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances
- other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual
- healthcare identifiers.

The full definition of health information, including exceptions, can be found in section 6 of the HRIP Act. Generally, any sharing of health information must be done in full compliance with the health privacy principles (HPPs) in the HRIP Act, unless one of the exceptions or exemptions under the HRIP Act applies or a Public Interest Direction or Health Privacy Code of Practice operates to provide an exemption. For more information on the HPPs see the IPC website.

When determining the type of data being requested you should also give consideration to whether the data is subject to the Dissemination Limitation Markers set out in the NSW Information Classification, Labelling and Handling Guidelines.

2.2 Identify whether your agency controls the data

Having identified the type of data being requested, you then need to determine whether this data is in the control of your agency. Section 6 of the Data Sharing Act authorises a government sector agency to share government sector data that it controls with another government sector agency or the DAC.

Your agency will have control of the data if:

- the agency has possession or custody of the data, or
- the agency has the data in the possession or control of another person or body. An example of this is where the data is in storage with a cloud storage provider.

Where your agency receives a request to share data that it has received from another agency, best practice would be for you to refer the request on to the agency which originally provided you with the data. Your agency may not have the relevant authority to release data provided to you by another agency.

2.3 Identify whether you can legally share the data

The next question you will need to consider is whether your agency is legally authorised to share the data.

The Data Sharing Act operates to authorise data sharing with another government sector agency for specific purposes. This Act operates to override secrecy provisions which are contained in other legislation, but does not override your obligations under privacy law. Where the sharing is compliant with the requirements of the Data Sharing Act, the provisions in legislation prohibiting disclosure of information obtained in connection with the administration of that legislation do not apply.[1]

[1] See section 5(1) of the Data Sharing Act

You will need to determine whether the data sharing request under consideration meets the purpose test under section 6 of the Data Sharing Act:

- to enable data analytics to identify issues and solutions regarding Government policy making, program management and service planning and delivery by government sector agencies
- to enable related government sector agencies to better develop Government policy making, program management and service planning and delivery by the agencies
- other purposes prescribed by regulation.

Any sharing under the Data Sharing Act must also be done in accordance with the PPIP Act, HRIP Act and any applicable Public Interest Direction or Privacy Code of Practice made under the privacy legislation

It should be noted that the Data Sharing Act does not authorise, permit or require the sharing of government data that is excluded information under Schedule 1 or Schedule 2 of the *Government Information (Public Access) Act 2009* (GIPA Act).[2] [3] Examples include Cabinet information, privileged information, information that is subject to secrecy provisions under specified legislation, etc.

In some circumstances data sharing for specific purposes is authorised by a Public Interest Direction or a Privacy Code of Practice made under the PPIP Act or HRIP Act. Further information on the PIDs and Codes currently in operation can be found on the IPC website.

If the data sharing request is made by an organisation or agency outside the NSW Government sector, you will need to consider whether your agency is authorised to share data in these circumstances. For example, some laws prohibit an agency from disclosing information obtained in connection with the administration of that legislation or may place limits on the organisations or persons with whom an agency can share data.

You will need to be aware of these restrictions before you undertake an assessment of a data sharing request. If you are unsure about whether your agency is subject to legislative restrictions on data sharing, you should seek advice from your agency's legal unit.

2.4 Identify the purpose for sharing the data

The next key consideration is the purpose for sharing the data.

The risks and benefits of sharing data will vary depending on how that data will be used and by whom. Statistical data which will provide input into the performance analytics of a specified program, for example, will carry a different set of risks than if that same data was intended to be used as easily-accessible test data for a prototype machine-learning system.

If you are sharing with a NSW government sector agency, then the purpose test under section 6 of the Data Sharing Act must be met before you can rely on the authority under the data Sharing Act (see section 2.3 above). If you are sharing with a non-government organisation, you should ensure that you understand the purpose for which the data is being requested.

---

[2] See section 5(2) of the Data Sharing Act.

[3] Clause 6 of Schedule 1 of the GIPA Act provides that it is to be conclusively presumed that there is an overriding public interest against disclosure of excluded information of an agency unless the agency consents to the disclosure.

Make sure that the sharing is for a specified purpose and that the purpose is understood by both parties. The formalisation of the agreed purpose in a data sharing agreement or memorandum-of-understanding is strongly encouraged as best practice and would be useful for future management and decision making.

At this stage of the process you should also consider the following matters:

Is the data fit for purpose?

Consideration should be given to whether the data requested are suitable for use in the manner intended by the requesting party. The data custodian will be able to advise whether the data is fit for the intended purpose and can provide you with a data quality statement.

For further information on data quality, see the NSW Government Standard for Data Quality Reporting.

2.5 Follow your agency's data sharing policy

Agencies may already have a data sharing policy in place. A data sharing policy is one which addresses the types of data agencies have in their custody, the principles and strategy around the sharing of that data and the governance and management procedures that should be followed when that data is being shared.

If the data requested is personal or health information, you should also review your agency's privacy management plan (PMP). The PMP should provide guidance on how your agency complies with the IPPs and HPPs, including collection, use and disclosure requirements. The PMP should be publicly available on your agency website.

2.6 Document your specific risks and mitigations

Once the type of data and the purpose of data sharing is determined, specific risk and mitigation strategies should be identified. In order to identify risks, consider any state-wide requirements or sector-specific requirements such as the agency's enabling legislation.

If the data requested includes personal or health information consider whether you should undertake a privacy impact assessment (PIA). A PIA can help you to identify and minimise privacy risks involved in a data sharing request. This will be especially important where the request involves sharing large data sets for linakge projects or unit-record level data.

The IPC has published a Guide to Privacy Impact Assessments in NSW that will assist you with this process.

Ensure that any mitigations that are to be applied to control risks are thoroughly documented in the data sharing agreement or MOU.

The following considerations should address the main areas of risk and help identify any appropriate mitigations.

Use considerations

It is important to consider the risks associated with how this data is intended to be used by the recipient. Regardless of data type, there are potential risks arising from instances where data is misused or mishandled. Consider the following questions when assessing potential risks:

- Is the proposed use of the data appropriate?
- What public benefit will it deliver?
- If the request involved personal information, could the same outcome be achieved with de-identified information?

- Does the proposed use involve using personal information for a purpose other than for which it was collected?
- Can the recipient be trusted to use the data appropriately?
- Does the recipient have the skills to analyse the data?
- Are there sufficiently robust governance arrangements in place to ensure that the privacy, confidentiality and security of the data will be maintained?

The following hypothetical case study is provided to illustrate how the use consideration may be applied.

Sharing data between government sector agencies

The Department of Education is developing a program to increase the rates of recreational fitness among public school students. In order to best target this program, the Department of Education has made requests to local councils to provide playground, aquatic centre and sports facility location information. The Department of Education intends to use this information to tailor the materials it is developing for schools to the particular facilities in each schools' local area. In return, the Department is sharing aggregated data with local councils about the number of students in their local government areas by age group and gender, which councils can use in their forward civil works planning.

The purpose of the data sharing in this instance is to enable better service planning and delivery, which is a permitted purpose under the Data Sharing Act. The Department of Education will develop a data sharing agreement between it and the councils involved which outlines their respective data govenrnance responsibilities as data custodians, thereby satisfying the safeguard requirements. After this has been developed, the data sharing is able to take place. This request is not dealing with information that identifies individuals and as such is not subject to the requirements in either the PPIP or HRIP Acts.

Commercial considerations

Data sharing could result in a breach of contractual or other commercial agreements. If you are dealing with commercially-sensitive data, consider the following questions:

- What parties are involved in collecting and using this data?
- Would sharing the data violate any existing contracts or commercial agreements?

Confidential, commercial-in-confidence or commercially sensitive information should be dealt with in a way that complies with any relevant contractual or legal obligations and does not affect the personal, professional, financial or commercial interests of an individual. It is usual for privacy requirements to be included in the relevant contractual arrangements.

You should seek advice from your agency's legal unit when considering a request to share data that may be commercially-sensitive or commercial-in-confidence.

Privacy considerations

If personal or health information is being shared by or with a public sector agency, the data sharing must be done in full compliance with the PPIP Act or the HRIP Act, unless one of the exceptions or exemptions under the PPIP Act or HRIP Act applies or a Public Interest Direction or Privacy Code of Practice operates to provide an exemption. The IPPs or HPPs must be complied with and appropriate privacy safeguards embedded in the data sharing agreement.

Will the sharing comply with the disclosure principle?

A public sector agency can only share (disclose) personal information if one of the exceptions under section 18 of the PPIP Act (or another exemtion under the Act) applies:

- the disclosure is directly related to the purpose for which the information was originally collected and the agency has no reason to believe the individual whose information is to be shared would object to it being shared
- the individual is likely to be aware or has been made aware that information of that kind is usually shared
- the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual or another person.

Note that different exceptions apply in relation to health information under the HRIP Act.[4]

Sharing personal or health information for purposes that were not disclosed to the individual when the information was collected may result in a breach of the PPIP or HRIP Acts unless one of the exemptions under Part 2 Division 3 of the PPIP Act apply or a Public Interest Direction or Privacy Code of Practice operates to provide an exemption.

There may be additional security or ethics requirements depending on the type of data being shared. For example:

- financial information, or other types of sensitive information, may require certain encryption standards
- approval from an ethics committee may be required where personal or health information is to be used for research purposes.[5]

Is consent required?

Determine whether consent is required from the individuals who are the subject of the personal information. If the information has not been de-identified and the individuals did not consent to data sharing at the time of collection, or if the shared data is being used for a purpose other than that for which it was collected, consent will generally be required (unless authorised by a Human Research Ethics Committee approval or by another law). Sections 17-19 and 26 of the PPIP Act outline the consent requirements for the use or disclosure of personal information.

Different consent requirements apply to health information and you should review HPP 11 to determine whether any of the listed exceptions apply in the context of the specific data sharing request.

Can access and correction processes be maintained?

Are there existing processes in place which allow people to update, correct or amend their personal or health information where necessary? These processes should be specified in the data sharing agreement and maintained for the life of the agreement. There are obligations in relation to amending personal information in section 15 of the PPIP Act and HPP 8 of the HRIP Act.

Can the appropriate storage and access controls be maintained?

The sharing agency should confirm that the recipient has the appropriate technical and physical controls in place to keep the data secure.

Section 12 of the PPIP Act addresses the retention and security obligations for personal information and HPP 5 addresses the retention and security obligations for health information.

[4] See Clause 11 of Schedule 1 of the HRIP Act (HPP 11) for further details of the exceptions that apply.

[5] For further information on the disclosure of personal or health information for research purposes, see the relevant IPC Statutory Guidelines available on the IPC website

Will 'sensitive' personal information be safeguarded?

Special restrictions apply to certain types of personal information under section 19(1) of the PPIP Act. This includes includes information about an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership.[6] An agency cannot share this type of personal information without an individual's express consent.

Generally, an agency can only disclose this personal information without consent where it is necessary to prevent a serious and imminent threat to any person's life or health, unless one of the exceptions under the PPIP Act applies or a Public Interest Direction or Privacy Code of Practice operates to provide an exemption.

Note that section 19(1) establishes a high threshold test which must be met before disclosure is permitted. Unlike some other exceptions under the PPIP Act (see for example section 18(1)(c)), section 19(1) requires that the disclosure be 'necessary to prevent a serious and imminent threat' rather than requiring that the agency 'believe on reasonable grounds' that the disclosure is necessary to prevent or lessen a serious or imminenet threat. This is an objectively higher threshold test to meet.

Will data be transferred to an organisation outside of NSW?

Transborder data flows involving personal or health information, including sharing data with Australian Government agencies, are only permitted in certain circumstances. These include:

- where the recipient is in a jurisdiction which upholds principles similar to those in the PPIP/HRIP Act
- where all individuals whose information is to be shared have consented to the sharing
- where the sharing is required for the conclusion or performance of a contract.

If you are considering sharing data that contains personal or health information across borders, ensure that you are complying with the requirements under HPP 14 or section 19(2) of the PPIP Act.

Additional considerations for health information

Further considerations should be taken into account when dealing with health information.

Is the data being shared for a secondary purpose?

Where health information has been collected for a specific purpose, it should not be shared for another purpose (a secondary purpose) unless a specific exception applies. The secondary purpose exceptions are set out in HPP 10 (use) and HPP 11 (disclosure) of Schedule 1 of the HRIP Act and include:

- the management of health services
- law enforcement purposes
- to lessen or prevent a serious and imminent threat to the life, health or safety of the person or another
- training or research purposes
- to locate a missing person.

[6] See section 19(1) of the PPIP Act

The exceptions under HPP 10 and 11 only operate in specific circumstances and you should consider seeking advice from your agency's legal unit or privacy contact officer before relying on one of the exceptions contained within the provisions. For example, in some circumstances you may be required to fully de-identify health information before sharing it with another public sector agency.

Where health information is shared in accordance with one of the secondary purpose exceptions, the recipient must not use or disclose the information for a purpose other than the purpose for which the information was given to them. The data sharing agreement should explicitly set out the purpose for which any health information has been shared, the permitted uses of that health information and whether the recipient may disclose the health information to a third party.

More information on the HRIP Act and permitted secondary uses can be found on the IPC website.

Does the data contain healthcare identifiers?

A healthcare identifier is a unique number that has been assigned to an individual patient or a healthcare provider for the purpose of managing or communicating health information.[7] An agency can only assign a healthcare identifier to an individual if it is reasonably necessary to carry out its functions efficiently.[8]

The sharing of health care identifiers is subject to the same disclosure rules as other health care information. HPP 11 in Schedule 1 of the HRIP Act sets out the principles governing disclosure of health infomation. The IPC recommends that you seek advice from your agency's legal unit or privacy contact officer before sharing data containing healthcare identifiers.

Does the data sharing involve linkage of health records?

HPP 15 must be complied with if the data sharing involves computerised linkage of health records. HPP 15 requires express patient consent if data sharing involves computerisied linkage of health records.

[7] The HRIP Act defines 'healthcare identifier' to have the same meaning as under the *Healthcare Identifiers Act 2010* (Cth).

[8] Clause 12(1) of Schedule 1 of the HRIP Act.

The following hypothetical case study is provided to illustrate issues for consideration when sharing personal and health information

Sharing Personal and Health Information

A university is conducting a research program into the impact of chronic health conditions on school performance and the effectiveness of early intervention programs. The research program intends to look at school attendance patterns and progression journeys for a cohort with specific chronic conditions.

The university has submitted requests to the Ministry of Health and the Department of Education seeking access to identified datasets about the cohort of students which contain their names, dates of birth and addresses, as well as the respective health and school performance information for each student. The university intends for the deidentified research findings to be provided to the agencies involved for their use in policy making, program development and service planning.

The purpose of the data sharing is to facilitate better policy making, program development and service planning. As the data involved contains both personal and health information, it needs to satisfy the requirements under the PPIP and HRIP Acts.

As an alternative to providing personal and health information, the agencies propose provision of the data after it has been through a linkage process to remove personal identifiers. Data linkage will enable the research team to identify school attendance patterns and progression journeys without revealing the identiy of the students in the cohort being studied.

A data sharing agreement is developed between the agencies and the research team that sets out the roles and responsibilities of each of the parties in relation to the handling of data.

2.7 Agency-specific considerations

The agency providing the data and the recipient must have in place the appropriate data custody and control arrangements to ensure that general data requirements are being adhered to. Your agency will have in place a records management program which ensures it meets its obligations under the *State Records Act 1998* (State Records Act), as well as compliance with obligations under the GIPA Act and the PPIP and HRIP Acts.

Also consider any relevant obligations in enabling legislation, agency-level data sharing policies, or privacy policies. Relevant contacts in your agency, such as the legal unit or the privacy contact officer, will be able to confirm whether there are additional agency or sector specific requirements that must be adhered to.

Questions you will need to consider include:

- Is the data sharing compliant with agency-level polices or enabling-legislation?
- What records are involved and will the records managements program obligations be complied with?
- Is the recipient of the data aware of these obligations?

2.8 Decide whether the data should be shared

Decisions around whether data should be shared should involve an evaluation of the risks involved with sharing the data. There are some situations where data should never be shared:

- where sharing would breach the disclosure principle under the PPIP Act or HRIP Act and no exceptions or exemptions apply
- if sharing with a non-government organisation, where this would breach any confidentiality or information sharing provisions under legislation applicable to the agency

- where the data requested is information subject to a conclusive presumption of an overriding public interest against disclosure (Schedule 1) or is excluded information (Schedule 2) under the GIPA Act and there has been no consent to disclosure by the relevant agency.

Contact the privacy contact officer in your agency to assist you in determining whether these circumstances apply.

Where the circumstances described above do not apply, consider the following questions:

- Does the use or disclosure of the information expressly relate to a proper purpose within the functions and responsibilities of the agency?
- If personal information will be shared, has the individual/s whose personal information is being shared consented or received appropriate notification of how your agency uses or discloses personal information?

Based on your knowledge of the data type, purpose for sharing, and the risks and mitigations associated with sharing, determine whether the benefits outweigh the risks of the data sharing for the specified purpose. If there are no further actions that can be taken to mitigte the risks, the data should not be shared. See Appendix 1 for a flowchart illustrating this process.

2.9 Exemptions and modifications to the IPPs/HPPs

There may be circumstances where there is a strong public interest case for sharing personal or health information, but no relevent exemption under the PPIP Act or HRIP Act authorises disclosing the information. In these circumstances consideration should be given to whether it would be appropriate to seek an exemption or modification of the relevant IPP/HPP to enable the sharing to occur.

The PPIP Act and HRIP Act both contain provisions for the making of a Public Interest Direction (PID) or Code of Practice. These are legal instruments which provide an exemption from, or make a modification to, an IPP or HPP. PIDs apply temporarily and are used for transitional or short-term purposes. Codes are intended for longer-term exemptions or modifications.

PIDs and Codes can only be made where there is a strong public interest case. A PID or a Code would only be appropriate for projects with a strong public benefit or where data sharing is necessary to provide services to the public.

Further information on PIDs and Codes can be found on the IPC website.

3. Preparing to share

3.1 Clarify the approval process

Once you have made the decision to share, it is good practice to clarify the approval process for the sharing of data. Your agency may have in place a standard approval process for sharing data.

The approval process should address the role and responsibilities of all agencies involved in the process.

3.2 Establish data governance arrangements

There should be formal documentation which sets out the data governance arrangements between the sharing agency and the recipient.

This documentation should set out the roles and responsibilities of both parties and address the specific requirements around the collection, storage, use, disclosure and disposal of the data. Specifically, it should include:

- the name and contact details of the sharing agency, the recipient of the data and their representatives
- the specific data that is being shared
- whether any personal or health information is being shared and the legal baasis 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.The data owner is a senior officer within the agency who is responsible for the quality of the data set.[9] Custodianship involves formally assigning rights and responsibilities for data and information assets, including capture and management on behalf of the NSW Government.[10]
- how the data will be shared
- how the data will be stored by the recipient
- how consent arrangements have been addressed - note that consent will only be applicable in some circumstances
- 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[11]
- any other obligations resulting from enabling legislation of either party
- the date, time and duration of the agreement.

The format this takes could be a memorandum-of-understanding or a data sharing agreement.

The Deparment of Customer Serice has developed a prototype Data Sharing Agreement Generator. Once fully operational, the Generator will provide a digital tool that NSW Government agencies can use to create or update existing data sharing agreements.

The Office of the National Data Commissioner has also published a data sharing agreement template that sets out the key matters that should be contained in a data sharing agreement. It should be noted that this is a general purpose template and does not address requiments under any specific legislative regime.

[9] For further information on the role and responsibilities of the data owner, see the Data Sharing Checklist for Data Owners prepared by Data.NSW.

[10] For further information see the NSW Data and Information Custodianship Policy

[11] See section 12 of the State Records Act for the records management obligations of public sector agencies.

3.3 Confirm the receiving environment

The sharing agency needs to be satisfied that the recipient has procedures in place to protect the data that are equivalent to those of the sharing agency.

The sharing agreement should detail how the recipient will receive the data and how it will be transferred and stored. This includes identifying any third-party or cloud providers that may be involved and the compliance of those third parties with data security standards (particularly if the cloud providers transmit or store data off shore); and ensuring that the recipient has appropirate safeguards in place to secure the data from unauthorised access by third-parties.[12]

The data recipient is responsible for ensuring that any obligations are met in arrangements where the received data is subject to data analytics work conducted by a third party, including the requirements that the data should only retained for as long as it is needed, subject to the requirements under the State Records Act.

3.4 Prepare the data for sharing

Before releasing data to another agency or organsiation consideration should be given to any treatment of the data necessary to control risk. Questions to consider during this process include:

Is all of the data relevant to the proposed purpose?

Sharing more data than is actually needed increases risks of unauthorised access and disclosure, so ensure that the data being shared is directly relevant to the agreed purpose. Consider exactly which data elements will need to be shared.

A best practice approach to data sharing involving personal or health information is to share data that is not identifiable where that data can meet the needs of the data user, and only share identifiable data if strictly necessary, and then in accordance with relevant privacy legislation.

Consider whether there are controls or treatments that should be applied to the data prior to release. For example, data minimisation, data aggregation, removal of direct identifiers or suppression of individual records.

Can the information be de-identified?

De-identification is a process that renders personal information into a form that is not identifiable.[13] Information that has undergone an appropriate and robust de-identification process is not personal information and therefore not subject to the PPIP Act or HRIP Act.

If possible, consider de-identifying information – including redaction where appropriate – before it is shared in order to protect the privacy of individuals and facilitate more secure data sharing.

There are risks of re-identification with any dataset. These risks may be hightened when a dataset contains small population sizes and when linking with other datasets. De-identification should not be the only mitigation strategy applied to protect against the risk of unauthorised disclosure of personal data. The IPC recommends that agencies seek expert advice in relation to complex de-identification matters.

More information on de-identification can be found on the IPC's website.

[12] See the NSW Government Cyber Security Policy for further details on

[13] For further information on de-identification see The De-Identification Decision-Making Framework published by CSIRO and Data 61 and Privacy-Preserving Data Sharing Frameworks published by the Australian Computer Society.

4. After you share

4.1 Oversight and auditing mechanisms

The governance documentation supporting the data sharing should state what ongoing auditing or monitoring processes will be in place to make sure obligations outlined in the data sharing agreement or other governance documents are being followed. The nature and duration of the data sharing will inform the focus and frequency of any auditing processes required.

The sharing agency should consider the following questions when determining the scope of audits and monitoring, especially when sharing personal or health information:

Is the data being used only for the purpose for which it was shared?

The auditing mechanisms established by the data sharing agreement should require the recipient to undertake regular audits of its use of the data to ensure that it is only used for the specfic purposes outlined in the agreement.

Are the access and storage arrangements secure?

The information should continue to be stored and accessed according to the standards agreed to at the time of sharing. Any changes to this should be communicated to and agreed to by the sharing agency. The specific retention and security obligations for personal information are set out in section 12 of the PPIP Act and HPP 5 of the HRIP Act.

Can individuals access their information?

If personal or health information is involved, there must be processes in place to explain to an individual what personal or health information about them is being stored, why it is being used, any rights they have to access it and processes in place which allow people to access their personal or health information without excessive delay or expense. This includes information about data that has been shared and what it is being used for by the recipient. These form part of the obligations under the PPIP (sections 12, 13 and 14) and HRIP (Division 3) Acts.

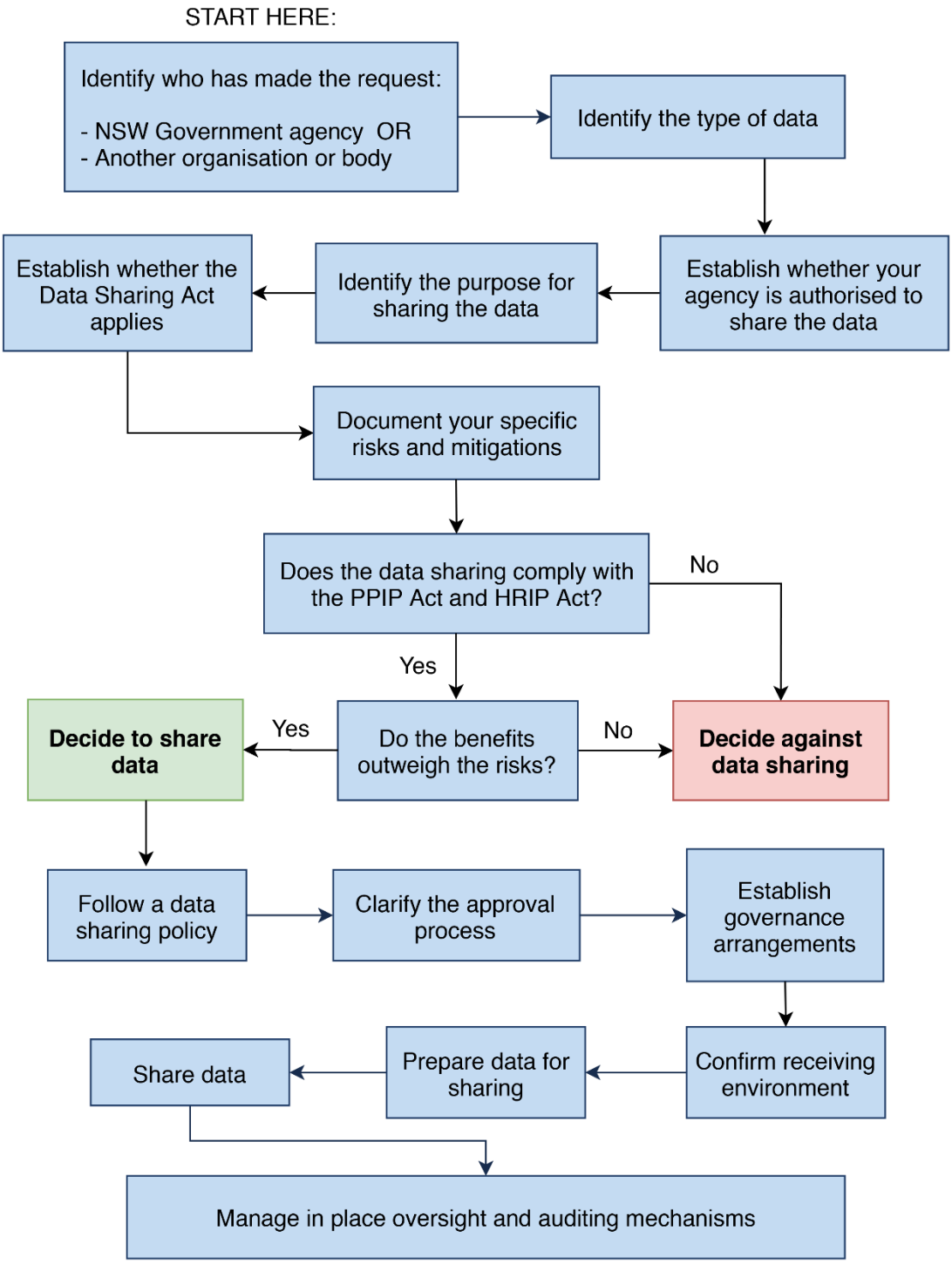
Are there processes in place for the information to be corrected?

There must be processes in place which allow people to update, correct or amend their personal information where necessary. The data sharing agreement should include a process by which the sharing agency will communicate any amendments or alterations to the data to the recipient. There are obligations in relation to amending personal information in section 15 of the PPIP Act and HPP 8.

Are there processes in place for the deletion or return of data?

The data sharing agreement should detail the requirements for deletion or return of data once the purpose for which it was shared is completed. Obligations in relation to retention and destruction of personal or health information are set out in section 12 of the PPIP Act and HPP 5.

5. Appendix A – Data sharing flowchart



Document information

Identifier/Title:	Data Sharing and Privacy
Business Unit:	Legal Counsel and Regulatory Advice
Author:	Senior Project Officer
Approver:	Privacy Commissioner
Date of Effect:	1 July 2020
Next Review Date:	July 2022
EDRMS File Reference:	18/5895/DJ
Key Words:	Data Sharing, Privacy, Personal Information, Health Information