



Australian Government
Office of the National Data Commissioner

SHARING DATA SAFELY





FOREWORD

Australia's data is a significant national asset, able to inform policy development, evaluate programs, contribute to economic growth and support innovation. Data driven innovation has been estimated to add up to \$64 billion per year to the Australian economy. Increasing the use and re-use of data has the potential to further contribute to economic growth and create jobs.

On 1 May 2018, I announced a suite of reforms in response to the *Productivity Commission Inquiry into Data Availability and Use*. The reforms include establishing new legislation to streamline data sharing and release while maintaining individuals' privacy and data security; and creating a new National Data Commissioner.

On 9 August 2018, I appointed Ms Deborah Anton as interim National Data Commissioner to lead our Government's public sector data reforms. The role of the National Data Commissioner is to ensure Australians benefit from data by making the sharing of public sector data safer, fairer and more transparent.

Government policy development, program implementation and service delivery can deliver greater benefits for Australian people and businesses using government data effectively and for that it is critical that Australians have trust in how government agencies use and share the data they collect.

This document outlines a set of five Data Sharing Principles, which government agencies can use to ensure that when they're sharing or releasing data, they retain a strong and consistent focus on individuals' privacy and data security.

These Principles and our data reforms more broadly will mean Government can harness the power of data to drive innovation while ensuring appropriate safeguards are in place to protect sensitive information.

The Hon Michael Keenan MP

Minister for Human Services and Digital Transformation

March 2019

GOVERNMENT AGENCIES ARE RESPONSIBLE FOR KEEPING AUSTRALIANS' DATA SAFE, BUT AGENCIES MUST ALSO MAKE THE BEST USE OF THE DATA.



Australian people and businesses provide data to government agencies every day, and those agencies are responsible for keeping the data safe and secure. Agencies are required to have safeguards in place to protect data – like legislation, secure buildings and IT systems, and strict requirements on employees who have access to data.

While it is important that agencies ensure data is safe and secure and is not accessed or used inappropriately, it is also important to make the best use of the data to improve government policies, services and programs.

There is substantial public benefit in sharing data and significant costs to Australians when agencies lock data away unnecessarily. It may be tempting to keep data locked away, but this can mean Australians are missing out on the significant economic and social benefits that can be realised if the data is shared safely between agencies, or with authorised expert researchers and analysts.

The five Data Sharing Principles outlined in this brochure are designed to help agencies share data safely and effectively, while keeping a strong focus on data privacy and security. The Principles support agencies to consider a range of factors, to help ensure the data is shared appropriately, with strong safeguards.

INTRODUCTION

The Government holds a wide range of data collected or generated by different government agencies. Agencies use data for a variety of purposes, including:

- informing policy development
- providing more tailored services to Australians
- evaluating the effectiveness of government programs
- ensuring compliance with laws and regulations
- protecting national security, and
- research and development to build a stronger economy and better society.

Data sharing can make it easier for government employees to do their jobs quicker, and with more accurate or up to date information, which means they can deliver better quality government services and programs to the community.

What is Data Sharing?

Data sharing is where agencies provide authorised users with access to data in a controlled manner.

Sharing and combining datasets can provide a richer picture of Australia's economy, society and environment, and significantly increase the value that agencies and researchers can obtain from separate datasets.

Agencies sometimes need to share data because one agency may not have the full range of data it needs to perform its functions, and accessing the data from another agency is quicker and cheaper than agencies collecting the data again themselves.

It's also easier for people and businesses if they can provide their information to one agency once, instead of giving the same information to several different agencies. This helps agencies reduce duplication of data across government systems and reduce costs.

Sharing data safely with researchers can also help address Australia's complex social and economic policy problems.

Not all data being shared is particularly sensitive, such as historical rainfall levels, flood levels or crop yields. When data sharing involves more sensitive information, such as people's income levels, or the locations of threatened species, or business profits and losses, the sharing needs to be managed carefully and responsibly.

CASE STUDY

MAKING NON-SENSITIVE DATA AVAILABLE TO EVERYONE



Where datasets are non-sensitive, they may be publicly released on **data.gov.au**

data.gov.au provides an easy way to find, access and re-use public datasets from different levels of Australian government.

data.gov.au provides access to over 70,000 different datasets, including:

- Energy rating data for household appliances
- Real-time information about fuel prices at service stations across New South Wales
- Locations of drinking fountains and public barbecues in the City of Melbourne
- Data on the number of people leaving or arriving in Australia
- Information on skill shortages in the Australian labour market, at the national and state or territory level.

Data sharing provides the opportunity for new and innovative purposes when that data is too sensitive to release publicly.

SHARING DATA SAFELY



THE DATA SHARING PRINCIPLES

The five Data Sharing Principles (The Principles) provide a framework for government agencies to share data safely. When agencies are considering whether there is public benefit in sharing data, they need to consider multiple factors, including:

- What project is the data going to be used for?
- Who is going to use the data?
- Will the data be used in a safe and secure environment?
- How detailed is the data?
- Can the results of the project be published without identifying the people or organisations that provided the data originally?

The Principles help agencies to think about all of these factors together and better manage any risks associated with data sharing.

If the joint protections offered by the Principles are not sufficient to protect against the risk of data breaches or data re-identification, then the data should not be shared.

The Principles will be applied differently depending on the context of the data sharing. Sharing data about business addresses requires different safeguards to sharing individuals' income data.

Each of the Principles allow for protections to be increased or decreased as required to ensure that in total the Principles provide for safe data sharing.

PROJECT PRINCIPLE

sharing data only for
appropriate
and
authorised
purposes

Government agencies may only share data for appropriate projects, where they are authorised to do so, and there are clear public benefits.

Agencies are only able to share data in clearly defined circumstances and where there is a clear public benefit from providing greater access to the data.

Sometimes agencies will have the permission of the individuals or businesses involved to share their data for specific purposes. For example, people undertaking a health survey may consent for the data to be shared with researchers doing work on a particular health concern; or businesses may agree that agencies can share data to save the businesses providing the same information to many different agencies.

Otherwise, the purposes for which agencies may share data are generally set out in relevant legislation. For example, data might be shared between agencies for the purposes of administering certain legislation.

Sometimes legislation will also spell out when data may not be shared. For example, data sharing may be prohibited if it would be a risk to the security, defence or international relations of Australia.

CASE STUDY

SHARING DATA TO MAKE BUSINESS REPORTING EASIER



Standard Business Reporting (SBR) is an approach to online or digital record-keeping that simplifies business reporting obligations. SBR is built into business and accounting software making it easier for business owners to report once to many different agencies. They don't need to spend hours filling out paper forms, re-entering information into different systems and portals, or working out what information is required for each specific agency.

The Australian Business Registry is responsible for SBR, and with the consent of business owners, is authorised to share data with the Australian Tax Office, the Australian Prudential Regulation Authority, the Australian Securities and Investment Commission, and State and Territory revenue offices.

PEOPLE PRINCIPLE

sharing data only with authorised users

An agency's decision on whether or not to share data with a particular user can depend on the user's ability to appropriately safeguard the data.

Government agencies may only share data with users who are able to use the data appropriately and keep the data safe.

Non-sensitive data, such as unemployment rates, can be publicly released, and made available for everyone to use. More sensitive data, such as address details, might be shared between service delivery agencies, because each of those agencies already has strong data safeguards in place.

Where researchers want to access particularly sensitive information such as de-identified health data to undertake health research, then the data might only be shared if the researchers have been vetted for suitability, and other controls are in place.

Users need to have the right skills and capabilities to safely use data.

It is critical that all data users have a clear understanding of what they can and cannot do with the shared data.

Users can be penalised for using data inappropriately or failing to keep data safe. In serious cases, these penalties can include fines, loss of employment or imprisonment.

CASE STUDY

LIMITING ACCESS TO AUTHORISED USERS



Data integration creates new datasets by linking data from different sources.

The Multi-Agency Data Integration Project (MADIP) links Census, tax, income support, education and health services data to support research and analysis.

Personal information, such as name and address, is removed so no identifying information is seen by the researchers using MADIP data.

Access to MADIP data remains tightly controlled. Only authorised government and academic researchers are granted access to the data for policy analysis, research, and statistical purposes in a secure environment.

Authorised researchers at the Australian National University are using MADIP data to better understand how the tax, welfare and health systems affect Australians. This project will provide deeper information for policy-makers on how location, age, and other social characteristics relate to income, support payments and health service usage of Australians.

SETTINGS PRINCIPLE

using data only in a
safe and
secure
environment

Government agencies need to ensure that data will only be accessed and used within an appropriately safe and secure environment.

A safe and secure environment incorporates requirements such as:

- Physically secure premises
- ICT systems protected from unauthorised access and cyber threats
- Training and stringent approval processes for individuals who are going to access the data
- Good data management processes and clear responsibilities
- Monitoring processes, such as reviews and audits.

CASE STUDY

A SECURE DATA ACCESS ENVIRONMENT



The Australian Bureau of Statistics (ABS) offers a secure IT environment for accessing data, known as the ABS DataLab. The DataLab is not connected to the internet and does not allow a user to copy information to any external device.

In addition to the IT protections, users who want to access data in the DataLab must complete a declaration of compliance with DataLab terms and conditions, and undertake mandatory training to ensure they understand their obligations when accessing the DataLab, how to safely access the DataLab and how to behave within the DataLab.

All activity in the DataLab is recorded, reviewed and subject to auditing. If an audit shows that a user has breached the DataLab conditions of use, the user's access may be withdrawn. If a user is responsible for a serious data breach they could face fines or imprisonment.

Authorised users access the DataLab for a variety of projects ranging from studies to determine the economic cost of dementia in Australia to research into Australia's future productivity growth.

DATA PRINCIPLE

applying appropriate protections to the data

Government agencies need to understand how sensitive their datasets are before they can make a decision on whether and how to share the datasets.

Some datasets are inherently more sensitive than others.

For example, data on air quality in Australia's cities is less sensitive – in general, this type of data should be safe to publish.

On the other hand, commercial-in-confidence data or data that can be used to identify specific businesses or individuals, is much more sensitive.

If different datasets are being combined, it's important to evaluate how sensitive the combined dataset would be. Agencies should consider what other datasets may already be publicly available. Sometimes combining datasets can make it easier to identify specific individuals or businesses. This can also happen if a dataset is considered alongside other information that is already public.

More sensitive data needs greater data protections under the other Principles than non-sensitive data. Data protections can include, data minimisation, aggregation, removing direct identifiers or suppressing individual records.

When data sharing involves sensitive personal information, like health data, the project may also need ethics committee approval before it can go ahead.

When sharing data, the basic rule 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.

CASE STUDY

ACCREDITED INTEGRATING AUTHORITIES: SAFELY LINKING SENSITIVE DATA



Data integration involves linking different datasets to create new datasets, which can provide information that has not previously been available. Some agencies are accredited to carry out data integration projects involving sensitive data. These accredited agencies have demonstrated that they can undertake data integration projects safely and securely.

Over the last few years, Accredited Integrating Authorities have undertaken data integration projects involving sensitive data such as combining Census data with migration data to understand the outcomes of people who have moved to Australia; and linking homelessness data with information about the use of drug and alcohol treatment services to understand the relationship between these two issues.

Releasing results from these data integration projects, or providing authorised users with secure access to integrated data, identifies patterns and trends in the Australian population and economy, and provides insights into the effectiveness of government policies, programs, and services.

OUTPUTS PRINCIPLE

ensuring public outputs from
data sharing projects

do not
identify

the people or organisations
within the data

Government agencies must put in place clear conditions of access and use to ensure that when results from data sharing projects are released, the identity of the people or businesses that provided the data remains private and confidential.

Agencies are not just responsible for the decision to share data with another agency or researcher; they are also responsible for what happens to the data after that.

A researcher investigating hospital admissions as a result of adverse effects of diabetes medication may have access to individual information to match up hospital records and pharmaceutical records for diabetic patients. However, when their research is published it will not be in any form that could be used to identify the individual patients.

Similarly, when the ABS collects data and publishes it in aggregate form as statistics in a table or chart, they make sure that the aggregation is done to a level where information about a specific individual or business can't be reasonably identified from the data.

CASE STUDY

ENSURING RESEARCH OUTPUTS PROTECT DATA PRIVACY



While many medicines can be lifesaving and life changing, patients can experience unexpected harmful effects after taking some medicines, or some combinations of medicines. Some adverse effects, such as heart failure, from using different medicines can be serious and life-threatening, but are also difficult to identify.

By linking Pharmaceutical Benefits Scheme data to health outcomes data, researchers were able to identify adverse effects not picked up through earlier clinical trials prior to the release of the medicines.

Researchers may need to access individual patient data to undertake this research, but the outcome of this study is then simply a list of medications with adverse side effects. The researchers do not publish individual patient data.

This research can help clinicians and regulators identify medicines or combinations of medicines that are unintentionally causing harm, and can potentially save Australians' lives.

OTHER OBLIGATIONS TO PROTECT DATA FROM MISUSE

The Data Sharing Principles can help government agencies decide if and in what circumstances they should share data. The Principles are an extra safeguard in addition to existing strong protections such as each agency's legislation, the *Privacy Act 1988*, security protocols, and other whole of government policies. There are strong penalties for unlawful sharing or release of data, or breaches of protocols and policies contained within specific legislation.

The Principles are being released in advance of the development of new data sharing legislation aimed at improving governance and transparency of Commonwealth data sharing.

PRIVACY

All Australian Government agencies are subject to the *Privacy Act 1988*, which regulates the handling of personal information about individuals. The *Privacy Act 1988* set out standards, rights and obligations for collecting, storing, using, providing access to, and correcting personal information.

- The Australian Government Agencies' Privacy Code requires government agencies to move towards a best practice approach to privacy governance to help build a consistent, high standard of personal information management.
- Entities, including government agencies, have data breach notification obligations when a data breach is likely to result in serious harm to any individuals whose personal information is involved in the breach.

SECURITY

All Australian Government agencies are subject to the requirements set out in the Australian Government Information Security Manual (ISM), which governs the security of government ICT systems. Agencies must also apply the Protective Security Policy Framework (PSPF) to safeguard ICT systems and mitigate common and emerging cyber threats. Employees who need access to classified information to do their jobs must also have an appropriate security clearance.

OTHER RELEVANT GOVERNMENT LEGISLATION AND POLICIES

All Australian Government agencies must also comply with a range of legislation and policies, including the *Public Service Act 1999*, the *Public Governance, Performance and Accountability Act 2013*, and the Commonwealth Risk Management Policy. Government employees must also abide by the Australian Public Service Values and Code of Conduct, declare any conflicts of interest, and may be bound by specific conditions of employment, depending on the type of work they do.

DATA SHARING AND RELEASE LEGISLATION

The Data Sharing Principles will also form a key component of the new Data Sharing and Release legislation being developed by the Office of the National Data Commissioner.



Copyright Statement

Sharing Data Safely © Commonwealth of Australia 2019

Copyright Notice

With the exception of the Commonwealth Coat of Arms, this work is licensed under a Creative Commons Attribution 4.0 International licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>)



Third party copyright

Wherever a third party holds copyright in this material, the copyright remains with that party. Their permission may be required to use the material. Please contact them directly.

Attribution

This publication should be attributed as follows:
© Commonwealth of Australia, Department of the Prime Minister and Cabinet, *Sharing Data Safely*

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the following website:

<http://www.pmc.gov.au/government/its-honour>.

Other uses

Enquiries regarding this document are welcome at:
information@datacommissioner.gov.au

