



Frameworks and Controls for Data Sharing



February 2023

About the editor



Dr Ian Oppermann FACS

ACS Immediate Past President

Ian currently holds the role of NSW Chief Data Scientist and is an Industry Professor at UTS. Ian has 30 years' experience in the ICT sector and has led organisations with more than 300 people, delivering products and outcomes that have impacted hundreds of millions of people globally. He has held senior management roles in Europe and Australia as Director for Radio Access Performance at Nokia, Global Head of Sales Partnering (network software) at Nokia Siemens Networks, and then Divisional Chief and Flagship Director at CSIRO. Ian is considered a thought leader on digital economies and is a regular speaker on big data, broadband-enabled services and the impact of technology on society. He has contributed to six books and co-authored more than 130 papers that have been cited more than 4,000 times. Ian has an MBA from the University of London and a Doctor of Philosophy in Mobile Telecommunications from the University of Sydney.

Foreword



If there's a lesson to be learnt from the last three years, it's that the management and protection of data has become a paramount concern for government and business.

In 2022, we saw enormous data breaches that affected the lives and identities of millions of Australians. Prior to that, we experienced an unprecedented need for data gathering and secure sharing during the COVID crisis, and we had to rapidly develop new systems and capabilities to share data at a velocity that we had never seen before.

Following these crises, reasonable questions are being asked about the use of data in our country. Are businesses and government gathering and holding too much data? Are we taking too many risks with the personal information of Australians? How should organisations be held accountable for breaches? And, critically, how can we continue to reap the benefits of data-driven decision-making and data sharing without creating unacceptable risks for the personal and private data of Australians?

The latter question is incredibly difficult to answer, and it's one we have struggled with in NSW Government for many years. I'm grateful to the ACS and to the many data scientists and IT professionals we have worked with over the years to help solve this problem.

Through my career in government, I've seen the benefits that shared data can offer. Our world-leading work on COVID tracking, on smart cities and urban planning, on providing unified access to government services – none of that would have been possible without robust frameworks that enabled us to share data safely and without risk to the identities of individuals.

The report you're reading now is the fifth and final in a series of papers ACS has produced on this subject, and I'm proud to note that I've been asked to be involved and help launch all five of them. This is critical work in the interests of NSW and Australia, and I hope it can serve as template for government and business to move forward and find answers to the wicked problems associated with data sharing.

The Hon Victor Dominello

NSW Minister for Customer Service and Digital Government, Minister for Small Business and Minister for Fair Trading



CONTENTS

Executive summary	4
Framework summary – structure of this paper	5
1. Introduction	6
2. So, you want to share or use data? – some problems	7
2.1 Every dataset is unique	7
2.2 There are many ways to ‘use’ data, and each data product is unique	7
2.3 The great handbrake is data quality	8
2.4 Revisiting personal information (PI) and personally identifiable information (PII)	10
2.5 Personal information from a spatial, temporal and relationship perspective	11
2.6 A reminder of the personal information factor	12
2.7 Sensitivity of data	13
3. Lenses to simplify data sharing	16
3.1 Data life cycle	16
3.2 Ways of accessing data	18
3.3 Virtualisation anyone?	19
4. Considerations for using data	20
4.1 Who wants access to the data and why?	20
4.2 Operational or non-operational	21
4.3 Potential harms	23
4.4 Principles of fairness and the relationship to data	24
4.5 Prohibition, restrictions and guidance for use	24
5. Bringing it all together	26
5.1 Application of controls based on risk – considerations and controls	26
5.2 Characterising levels of control	26
5.3 Determining the level of control required	29
5.4 What about people?	29
5.5 Moving between layers of control	30
6. Discussion	33
6.1 The work on PIF is continuing – OptimShare	33
6.2 Advances in data and digital standards	34
7. Conclusions	36
8. Thanks	37
9. Appendix – building a dataset in action	38

Executive summary

This paper is the last in our series of efforts to identify frameworks that can be used to safely share and use data. It is a refinement of the 2021 white paper *Sharing Data in Trusted Frameworks*, which introduced frameworks and controls for data sharing that consider the level of personal information in data, sensitivities associated with the use of the data itself, and sensitivities in use of outputs of analysis of data.

These sensitivities are addressed by variable controls at appropriate points in the data life cycle. This final paper in the series builds on white papers published in 2017, 2018, 2019 and 2021.

The work identifies controls to ensure that data is treated appropriately along its life cycle. It is this, often unknown, life cycle that creates so much concern for data custodians and others involved in the data ecosystem, including data subjects themselves.

The controls identified in this paper are linked to demonstrated capability, assessable governance, and clear authority at each phase of the data life cycle. These link the purpose of data sharing (the 'why') with the mode of data sharing (the 'how') and provide a method to ensure sufficient governance in the circumstances.

Key messages

- Not all data is the same. Except in extreme cases, the level of personal information in a dataset cannot be systematically measured, and the inherent sensitivity of data itself, or the use of the data, cannot be unambiguously assessed. Data quality is also not able to be systematically assessed against an intended use case except in extreme cases.
- The consequences are multiple:
 - most people-centred data, even if de-identified through removal of unique identifiers, is treated as if it were personally identifiable information
 - many data custodians are concerned about the fitness of purposes of data for target use cases
 - many data custodians are concerned about the unintended consequences of release or use of data.
- The situation is compounded by existing state and Commonwealth privacy legislation, which refers to personal information as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable'.
- The complexity of data life cycles is also identified as a limiting factor for systematic data sharing, as is the rising concern around cyber security where unintended and unauthorised users access data for their own means.
- This paper attempts to identify conditions required to be in place before data is used, considerations for use, and guidance around further use of data products as they are on-shared. It also briefly touches on alternatives to creating datasets that create cyber security challenges.

Framework summary – structure of this paper

This paper walks through the various elements that must be factored in when planning risk management over the life cycle of a shared dataset. It is a loosely structured framework that covers the various considerations of a safe dataset and how to manage those risks. It builds upon previous ACS white papers that cover the individual issues in more depth:

- *Data Sharing Frameworks* (2017)¹
- *Privacy in Data Sharing: A Guide for Business and Government* (2018)²
- *Privacy-Preserving Data Sharing Frameworks* (2019)³
- *Sharing Data in Trusted Frameworks* (2021)⁴

Chapter 1 introduces the topic that needs to be solved, building on the work of the 2021 white paper.

Chapter 2 presents an overview of core challenges when wanting to use or share data.

Chapter 3 provides a number of simplifying lenses to assist the development of data sharing frameworks and inform the controls applied at each stage of the data life cycle.

Chapter 4 examines major elements to consider when using or sharing data. As the data moves through its life cycle, the sensitivities, and therefore required controls, must change.

Chapter 5 brings it all together and looks at how you can take these elements and develop a unified plan for data-sharing controls over the entire life cycle of a dataset. At the end, you should have a usable framework for the application of controls on the data, which will guide decision-making on the safety and usability of the data. An example of a control track can be seen in Figure 1 below.

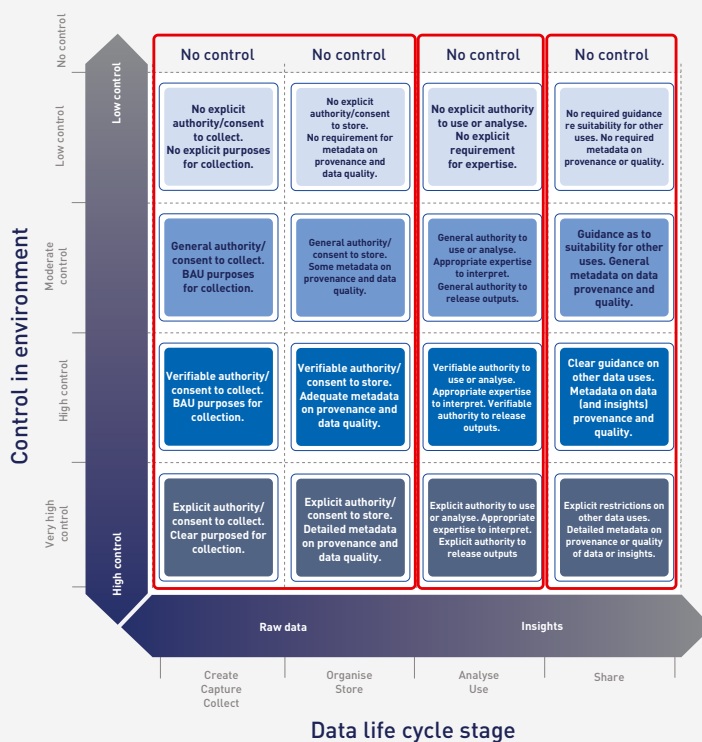


Figure 1: Characterising control layers through the data life cycle

1 Available at <https://www.acs.org.au/insightsandpublications/reports-publications/data-sharing-frameworks.html>
 2 Available at <https://www.acs.org.au/insightsandpublications/reports-publications/privacy-in-data-sharing.html>
 3 Available at <https://www.acs.org.au/insightsandpublications/reports-publications/privacy-preserving-data-sharing-frameworks.html>
 4 Available at <https://www.acs.org.au/insightsandpublications/reports-publications/sharing-data-in-trusted-frameworks.html>

1. Introduction

Sharing Data in Trusted Frameworks highlighted the real-world complexities of data sharing and use. Except in extreme cases, the level of personal information in a dataset cannot be systematically measured, and the inherent sensitivity of data itself, or the use of the data, cannot be unambiguously assessed.

Data quality also cannot be systematically assessed against an intended use case except in extreme cases. The consequences are multiple and ultimately complicate data sharing. Firstly, most people-centred data, even if de-identified through removal of unique identifiers, is treated as if it were personally identifiable information, greatly restricting who has access and for what purposes. Secondly, the inability to systematically access data quality in a way that is suited for individual use cases leaves many data custodians concerned about the fitness of purposes of data.

Finally, many data custodians are concerned about the unintended consequences of release or use of data, partly due to the lack of control over how a data product (for example, an insight, a report, a comparison or an alert) may be used or re-used. This last point is complicated by the complexity of data life cycles, which extend beyond the simple exchange of data (or data products) between two parties.

The complexity of data life cycles was identified in *Sharing Data in Trusted Frameworks* in terms of the inability to apply controls to the further use of data (or data products) beyond the simple cases of 'no control' or 'very high control'. Respectively, these effectively open data up to the entire community (open data) or greatly restrict it to a very small number of users (closed data).

The situation is compounded by existing state and Commonwealth privacy legislation, which refers to personal information as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable'. The inability to determine who is reasonably identifiable within a dataset often drives extreme caution.

Cyber security is also an emerging factor in the consideration of how (or even if at all) datasets should be created for general use. At the time of writing, major breaches of customer data have led to escalated calls for the reduction of data that is collected, and for how long individual data is held.

This critical question addressed in the 2021 white paper is whether all the possible ways of accessing and using data, including sharing and analysis, can be mapped to a finite number of repeatable frameworks that consider:

- tracing and assessing the chain of authority to receive and use data
- following the flow and use of data in digital or non-digital formats
- capturing and enhancing the metadata on provenance and consent (or permission) to process and on-share
- capturing and enhancing the metadata on data quality
- following the impact on the data itself as it moves between entities.

This paper extends the simple frameworks introduced in the 2021 white paper to expand and integrate the key elements into an overarching ecosystem. The goal is to develop practical data sharing frameworks, with identifiable controls, that operate in practical environments. Examples are also provided through the paper.

This paper assumes all analysis is performed using data that has been de-identified, meaning the data has no unique identifiers. It is also assumed that the de-identified data is not subject to any national security classification.

2. So, you want to share or use data? – some problems

It is sometimes conceptually convenient to think of data as having a simple, linear life cycle, with a data analysis, or other single use at the centre of that life cycle. In practice, data can be used and re-used many times. It can pass through many hands, or algorithms; be used to generate insights; or be combined with other data and insights. Copies of the data and associated metadata and insights can be recombined or archived. The unknown nature of the total data life cycle, and the lack of controls that can be activated or scrutinised by data custodians can lead to a culture of hesitancy to share data.

The dilemma often faced by people who want access to data is how to build a trusted data sharing framework in the absence of one. The question of 'Can I have access to your data?' will very often be met with a firm, polite but negative response of 'No', often backed by the statement 'because of the Privacy Act' – the BOTPA reason. This is particularly true if the data is about people.

Ultimately data sharing is an act of trust, and trust is either developed within a trusted relationship or through demonstration of trustworthy capability that encompasses technical and governance capability, as well as authorisation frameworks and clarity of purpose. Data sharing and use is not a single transaction, but parties who share data are a step in what may be a very complex data life cycle. As the number of stages of the life cycle increase, trust between parties becomes increasingly difficult to maintain. Trust between parties can be replaced with controls and scrutiny to ensure appropriate use of data across the stages of the data life cycle.

It is important to realise that a few home truths about data sharing.

2.1 Every dataset is unique

It may come as a surprise, but it is arguable that every dataset created or collected is unique in a number of ways. It is these unique elements that make dealing with data in a generic way so challenging.

Some of the elements that make datasets unique:

- every dataset is a record of some thing or event(s) in the past
- every dataset has finite precision

- every dataset is created in a unique context (when, where, over what period of time, by whom or what)
- every dataset has a unique history of handling, access and use.

Even when datasets are copied, the copies have their own unique history handling, access and use. The subject of the data also has an inherent sensitivity and, for people centric data, has a level of personal information embedded.

If the unique elements of the dataset are captured in the form of metadata, then appropriate handling and use of the data becomes more tractable.

2.2 There are many ways to 'use' data, and each data product is unique

When data is used, its unique history is changed, and the 'product' of that use has its own unique history for the same reasons described above.

The range of data products is very wide and can include a chart, an insight, a modified version of the data, an alert, an alarm, a decision or an action.

A useful way to think about data products is as operational and non-operational products. Operational data products seek to make a difference in the real world, driving a response or initiating an action.

A non-operational product may surface information from data but will not directly impact a real-world outcome.



2.3 The great handbrake is data quality

In surveys of data custodians and the general public, the intended use of the data was frequently identified as a very significant factor when determining the risk framework for data sharing and use.

Data quality underpins many of those concerns about data being released for use, ranging from concerns about the data reflecting poorly on the data custodian to concerns about poor-quality insights or data products being generated from poor-quality input data. If the data quality is not known, then appropriate care may not be taken with data products or insights generated, and how they are used.

Part of a data sharing risk framework includes consideration of the data quality and if that quality is fit for the intended use. Data quality is often described as consisting of four dimensions: accuracy, timeliness,

completeness, and consistency. For each dimension, it is important to understand the impact of high, medium or low values of that data quality dimension. It is also important to then understand the cumulative effect of the impact of several data quality dimensions.

An overall assessment can then be made against the use case. For example, the accuracy of an algorithm may be very sensitive to accuracy of data, or the value of a benchmark may be only slightly sensitive to the timeliness of a dataset. Finding appropriate ways to assess the sensitivity of a use of data against each data quality element is critical to providing the right guidance, restrictions or even prohibitions on how a dataset may be subsequently used, or how a data product may be relied upon.

Quality dimension	Sensitivity associated with high values of this quality component	Sensitivity associated with moderate values of this quality component	Sensitivity associated with low values of this quality component
Accuracy	Low	Medium	High
Timeliness	Low	Medium	High
Completeness	Low	Medium	High
Consistency	Low	Medium	High

Sensitivity of dataset defined by highest level of any subject covered by dataset (min-max)

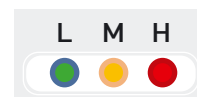


Figure 2: A simple framework to consider the risks associated with data quality

In the 2021 white paper, a more general two-layer data quality standard with detailed data quality indicators was identified from independent research.⁵

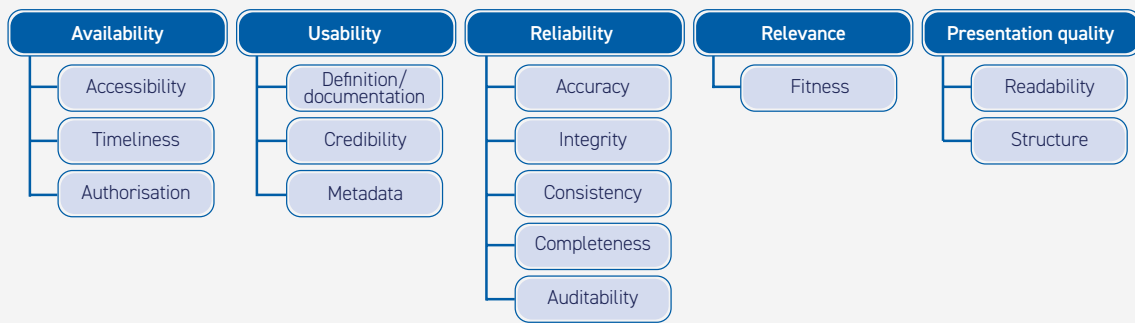


Figure 3: Data quality framework

This data quality framework is composed of five dimensions of data quality – availability, usability, reliability, relevance, and presentation quality. For each dimension, the authors identified one to five elements to quantify data quality. The first four quality dimensions are regarded as indispensable, inherent features of data quality and the final dimension is additional properties that improve ease of use. The characteristics of these five dimensions can be seen below:

- Availability is defined as the degree of convenience for users to obtain data and related information, which is divided into the three elements of accessibility, authorisation, and timeliness.
- Usability refers to whether the data is useful and meets users' needs, including data definition/documentation, data reliability and metadata.
- Reliability refers to the level of trust in the data; this consists of accuracy, consistency, completeness, adequacy, and auditability elements.
- Relevance is used to describe the degree of correlation between data content and users' expectations or demands; adaptability is its quality element.
- Presentation quality refers to a valid description method for the data, which allows users to fully understand the data. Its dimensions are readability and structure.

The International Standards Organisation JTC 1's subcommittee 42 on artificial intelligence (AI) is working on draft standards in the form of 'ISO/IEC AWI 5259-1 Artificial intelligence – Data quality for analytics and machine learning'.

In the meantime, data quality can be assessed against the intended use. For some data uses, the data quality can be described in relative terms. Some trivial examples:

- Analysis type: count (histogram, PDF, CDF, benchmark)
 - Data quality requirements: the data field to be counted must be accurate to within counting limit of resolution. Other quality parameters limit use of analysis.

- Analysis type: thresholding, discriminator, classifier
 - Data quality requirements: the value of the data field to be classified must be closest to the correct class value within the classification limit of resolution. Other quality parameters limit use of analysis.
- Analysis type: prediction
 - Data quality requirements: data quality limitations incrementally impact the principal components of the prediction. The data quality of the principal components must be improved to improve algorithm accuracy. Other quality parameters limit use of analysis.

5 Cai L and Zhu Y (2015) 'The Challenges of Data Quality and Data Quality Assessment in the Big Data Era', Data Science Journal, 14:2, <http://doi.org/10.5334/dsj-2015-002>

2.4 Revisiting personal information (PI) and personally identifiable information (PII)

The 2019 (*Privacy-Preserving Data Sharing Frameworks*) and 2021 (*Sharing Data in Trusted Frameworks*) white papers repeatedly addressed the issue of the level of personal information in a linked, people centric dataset and presented a tool for measuring the level of PI through a personal information factor (PIF).

Despite the advance of years, the concepts of personal information versus personally identifiable information remain not clearly differentiated in regulatory frameworks and even in common language. The term 'personal information' is typically used very broadly and is described differently in different parts of the world. The guidance on the website of the Office of the Australian Information Commissioner remains:⁶

Personal information is information that identifies or could reasonably identify an individual.

The *Privacy Act 1988* and the *Freedom of Information Act 1982* define 'personal information' in the same way:

Personal information means information or an opinion about an identifiable individual, or an individual who is reasonably identifiable

- a. whether the information or opinion is true or not and
- b. whether the information or opinion is recorded in material form or not.

While not uniquely identifiable, eye colour, hair colour and shoe size are all PI (information about an identifiable person). The threshold question is then: when is the person identifiable?

This begets the question: can this threshold of PII and the definition of 'reasonable' be quantified? The answer depends on context.

Some of the relevant dimensions of this context are:

1. Can an individual in a dataset (rows of people and columns of features) be identified as unique, based on a single feature or combinations of features?
2. Can the unique row be identified in other datasets and so link information between datasets (for example, unidentified online browsing records)?
3. Can the unique row of features be mapped to an actual person or small group of people, based on access to other data?
4. Could someone observing the unique row spontaneously identify the actual person from the unique feature or feature combination, based on their own knowledge?
5. Is an individual known to be in a dataset, and could their row be identified based on a subset of features?
6. Is an individual known to be in a dataset and knowledge the nature of the dataset (for example, patients with cancer) lead to inferred information about an individual?

A similar logic can apply to a small number of rows with the same feature values. Being able to narrow down to a small number of identical rows may introduce some uncertainty, but many of the contextual considerations above remain relevant.

These contextual considerations require different controls for different environments to preserve privacy and avoid PI becoming PII. This includes screening who has access to data, controlling access to linkable datasets and providing prohibitions on use (and secondary use) of data and data products.

⁶ Available at <https://www.oaic.gov.au/freedom-of-information/frequently-asked-questions/what-is-personal-information-and-how-does-it-interact-with-the-freedom-of-information-act-1982/>

The previous ACS white papers demonstrate the simple concept that the level of PI in a linked, de-identified dataset increases as more people-centred datasets are linked. Conceptually shown in Figure 4, as more datasets containing PI are linked, a point may be reached where an individual is personally identifiable, or 'reasonably' identifiable. The dataset is then considered to have PII. The epsilon in this figure is an indication of the difference represented by the gap before the 'reasonable' threshold is met.

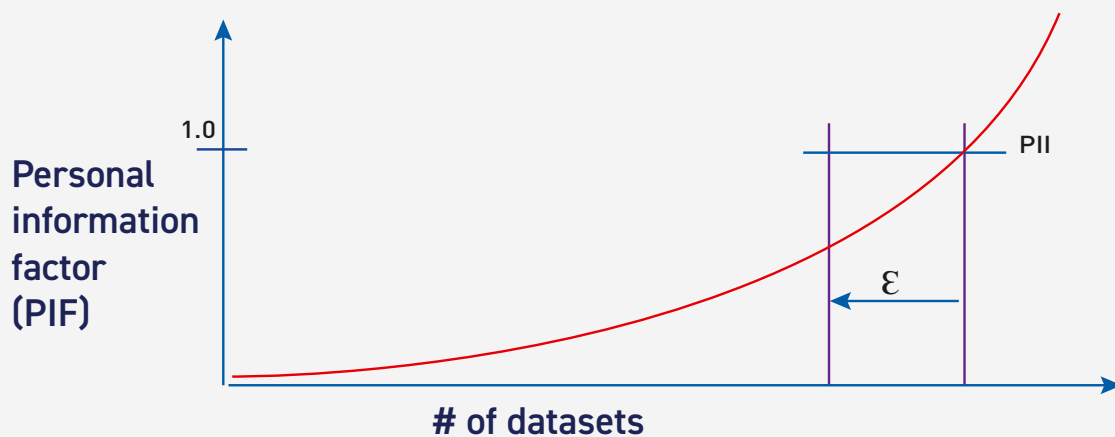


Figure 4: Conceptualisation of a normalised personal information factor (PIF) and the threshold point of reaching personally identifiable information (PII)

2.5 Personal information from a spatial, temporal and relationship perspective

All data about people is captured 'somewhere' and at 'some time'. Even if location and time are not explicitly recorded in a dataset, it may be reflected in the metadata, which is 'data about the data'. What is also often captured is the 'relationship' of a person in a dataset to an object, event or other person. For example, if a transport card was tapped to allow someone on to a train, the time and location of the ticket barrier is known (and may be recorded in the data) as well as the fact that a person interacted with a particular ticket gate. Again, even if not captured in the end dataset, it can be known from the metadata about the event – the 'tap'.

If you were a detective trying to identify a suspect in a murder case, you would seek to place the suspect in the vicinity (space) at the time of the murder (time) and

in the proximity of the victim (relationship). If you were trying not to identify an individual (that is, to protect their personal information from re-identification), the dimensions of temporal, spatial and relationship parameters could be separately protected. This would include taking care that the minimum identifiable cohort size (MICS – the smallest number of individuals with the same values for features) in any of the temporal, spatial and relationship parameters was above a predetermined threshold. This concept is shown in Figure 5 over the page.

What is important to understand from this figure is that the level of personal information, or the sensitivity of that information, can be differently viewed from the lens of time, space and relationships. The sensitivity of data will be addressed later.

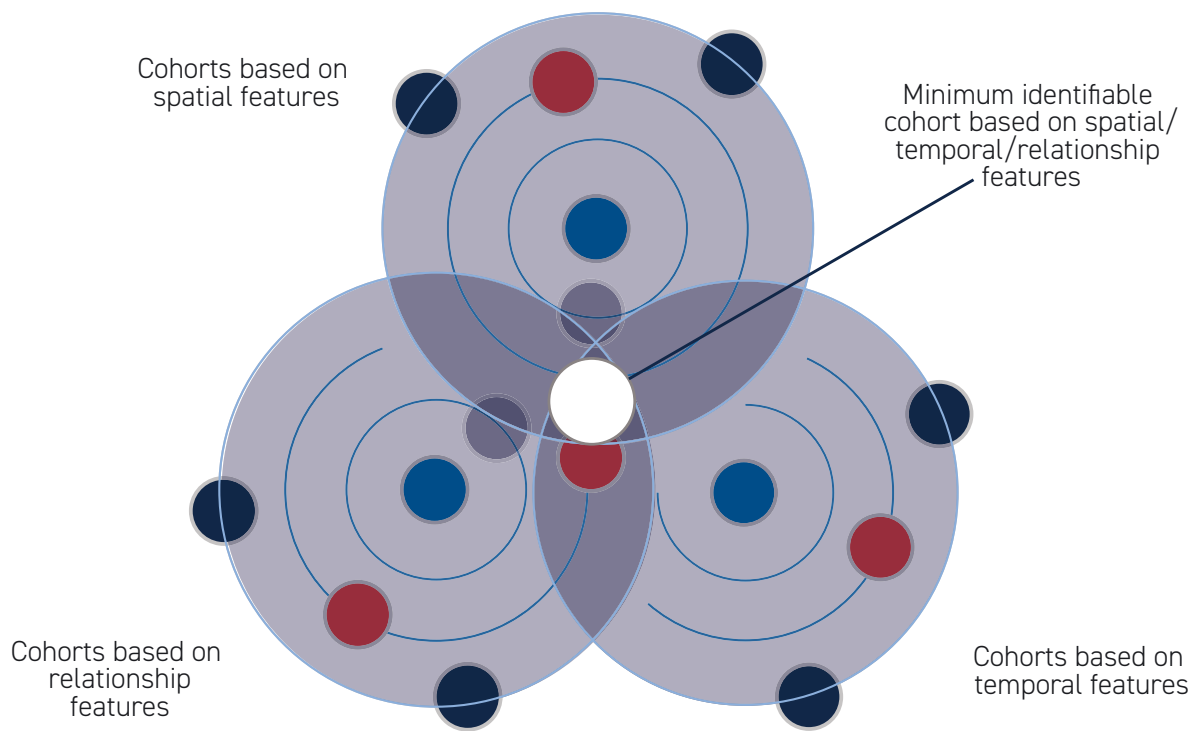


Figure 5: Identifying minimum cohorts based on temporal, spatial and relationship parameters

2.6 A reminder of the personal information factor

A fundamental concept covered in the ACS technical white paper Privacy-Preserving Data Sharing Frameworks was a way to calculate an important parameter, a 'personal information factor' (PIF), which is the measure of information gain an 'attacker' would gain for an individual known to be in a dataset (rows of individuals and columns of features). The information gained for any given feature for the known individual was

referred to as the 'cell information gain' (CIG). The sum of all of the CIGs for a row became the 'row information gain' (RIG). The PIF for the dataset was defined to be the highest RIG within the dataset when normalised by the number of rows that were identical with that RIG. This meant that, if one row was unique and had the highest RIG, it determined the PIF for the dataset.

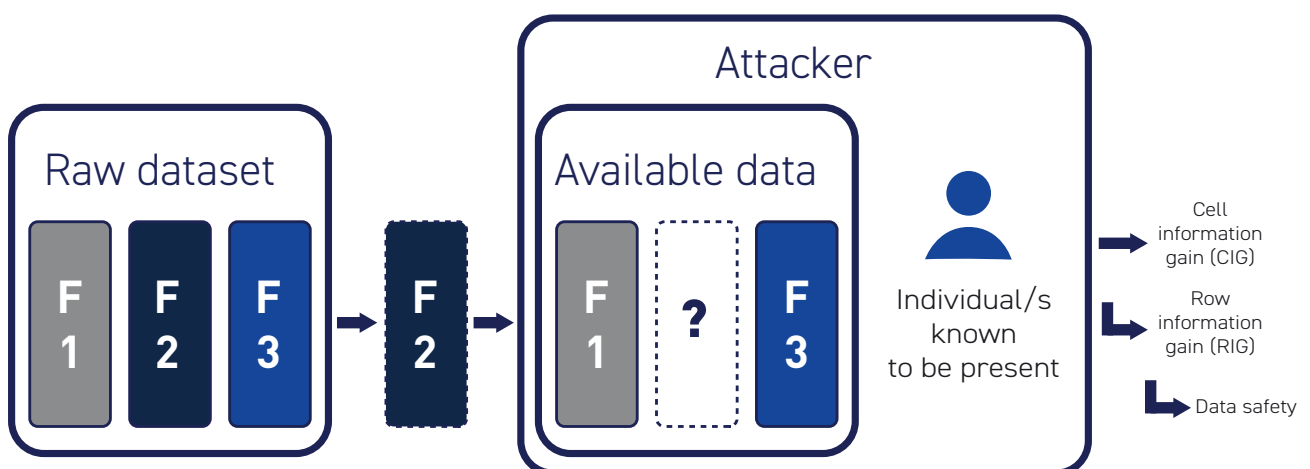


Figure 6: Conceptual model for information gain by an attacker

Excerpt from the 2019 white paper *Privacy-Preserving Data Sharing Frameworks*:

The PIF for the dataset is driven by both the minimum identifiable cohort size (MICS) and the amount of information that would be revealed if individuals in this cohort were re-identified. The definition of PIF is still a work in progress, but the current working definition is given as:

$$\text{PIF} = \text{maximum of } (\text{RIG}_{(x)} / (\text{MICS at } \text{RIG}_{(x)}))$$

At any given RIG threshold, the MICS at that value is the smallest number of rows with the same column values. For example, if the number of rows with a RIG at RIG_{max} is 1, then the PIF is equal to RIG_{max} . If the number of rows with a RIG of RIG_{max} is 2, and there are no other unique rows in the dataset, then the PIF is $\text{RIG}_{\text{max}} / 2$. If there is a unique row at a threshold RIG less than RIG_{max} (for example, $\text{RIG}_{(x)}$) and the number of rows at is RIG_{max} is 2, then the PIF is $\text{RIG}_{(x)}$ provided $\text{RIG}_{(x)}$ is greater than $\text{RIG}_{\text{max}} / 2$.

2.7 Sensitivity of data

It seems intuitively obvious that the subject of data can be inherently sensitive. Quantifying just how sensitive is again a subjective matter. Under the Commonwealth *Privacy Act 1988*, sensitive data is of greater importance in terms of confidentiality, in particular where it leads to worse consequences for a re-identified individual. The Office of the Australian Information Commissioner (OAIC) offers examples of sensitive data subjects.⁷

Sensitive information is personal information that includes information or an opinion about an individual, including their:

- racial or ethnic origin
- political opinions or associations
- religious or philosophical beliefs
- trade union membership or associations
- sexual orientation or practices
- criminal record
- health or genetic information
- some aspects of biometric information.

What is less obvious is the sensitivity of data when viewed through the lens of time, space and relationships. For example, data that contains criminal record information is sensitive according to the list from the OAIC. This data may be required to be

protected through aggregation or perturbation (creation of a new, less personally identifiable data product) if it is to be released for wider use.

Data that contains criminal record information is arguably more sensitive if it also contains address data. Even if protected through aggregated before wider use, the ability to infer criminal record information at a postcode level arguably creates a sensitivity that would not be present were spatial information not present.

Figure 7 below takes the example parameters from the OAIC and suggests consideration of the level of sensitivity of each parameter in the context of:

- High spatial or temporal or relationship parameter resolution – specifically seeking to test the view of sensitivity of that parameter if any of the three dimensions were fine-grained.
- Moderate spatial and temporal and relationship parameter resolution – specifically seeking to test the view of sensitivity of that parameter if all three dimensions were moderately fine-grained.
- Low spatial and temporal and relationship parameter resolution – specifically seeking to test the view of sensitivity of that parameter if all three dimensions were not fine-grained.

⁷ See <https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-personal-information#SensitiveInfo>

This consideration framework does, of course, avoid several difficult questions including:

- What is meant by fine-grained, moderately fine-grained and not fine-grained resolution?
- What is the treatment if more than one sensitive subject is included in the dataset; for instance, do two moderate sensitivities equate to a high sensitivity?
- What additional information or risk is created when multiple sensitivity subjects interact?

For instance, does knowing children and criminal record and ethnic origin (all with low sensitivity) create a greater sensitivity that simply having '3 x low', because of some other real-world potential inference between these parameters?

These questions need to be carefully considered when using data or creating data products, even if the data products are aggregated versions of the original datasets.

Data subject	High spatial <i>or</i> temporal <i>or</i> relationship resolution	Moderate spatial <i>and</i> temporal <i>and</i> relationship resolution	Low spatial <i>and</i> temporal <i>and</i> relationship resolution
Children	High	Medium	Low
Minorities	High	Medium	Low
Religious or philosophical beliefs	High	Medium	Low
Racial or ethnic origin	High	Medium	Low
Political opinions or associations	High	Medium	Low
Trade union membership or associations	High	Medium	Low
Sexual orientation or practices	High	Medium	Low
Criminal record	High	Medium	Low
Health or genetic information	High	Medium	Low
Personal biometric information	High	Medium	Low

Sensitivity of dataset defined by highest level of any subject covered by dataset (min-max)



Figure 7: Considering data sensitivities in the context of spatial, temporal and relationship dimensions



3. Lenses to simplify data sharing

It is sometimes conceptually convenient to think of data as having a simple linear life cycle. The real world shows us that, once created, data and data products may be used (and re-used) many times in many forms. This makes identifying a simple series of controls that are effective over such an elongated life cycle a significant challenge. Nonetheless, the simple linear life cycle can help identify where to start.

3.1 Data life cycle

In an evolution from the 2021 white paper, Figure 8 shows a simplified data life cycle that allows us to explore controls that may be considered from the point of data creation to collection, storage and then use by the receiving entity. The complexity of real-world data life cycles makes the simple linear model more likely to be an exception rather than the general model.

Figure 8 focuses on **access** to, **use** of, and **sharing/archival** of data, with the implications of repeated access to data (and metadata and insights), use of data (and metadata and insights), and sharing of data (and metadata and insights).

This 'use' may be analysis of the data. The data or data products are then shared and finally archived. The simple life cycle can be expanded at any phase to more explicitly show the range of activities that take place during that phase. Along the way, the original data is assumed to be modified from its original form – from when it was captured (D_1), transmitted (D_2), stored (D_3), used (as D_4) and then stored (as D_5).

The types of factors that can impact data during these stages include:

- subsampling of raw data or reduction in data precision before transmission
- loss of data, lossy data compression⁸ or data corruption during transmission
- loss of data, lossy data compression or data corruption during storage
- lossy data decompression or data corruption when importing data, removal of low-quality data before use
- loss of data, imperfect data compression or data corruption during archiving.

As a consequence, the data that is finally 'used' may well be different from the data that was originally created or collected. In modern digital information management systems, data loss and corruption are rare. However, if data is captured from a camera on a drone, transmitted wirelessly and then compressed on storage before analysis, many more data loss or data quality events may occur. Once data is used, an incomplete dataset may then ultimately be archived.

⁸ In information technology, 'lossy compression' or irreversible compression is the class of data encoding methods that uses inexact approximations and partial data discarding to represent the content.

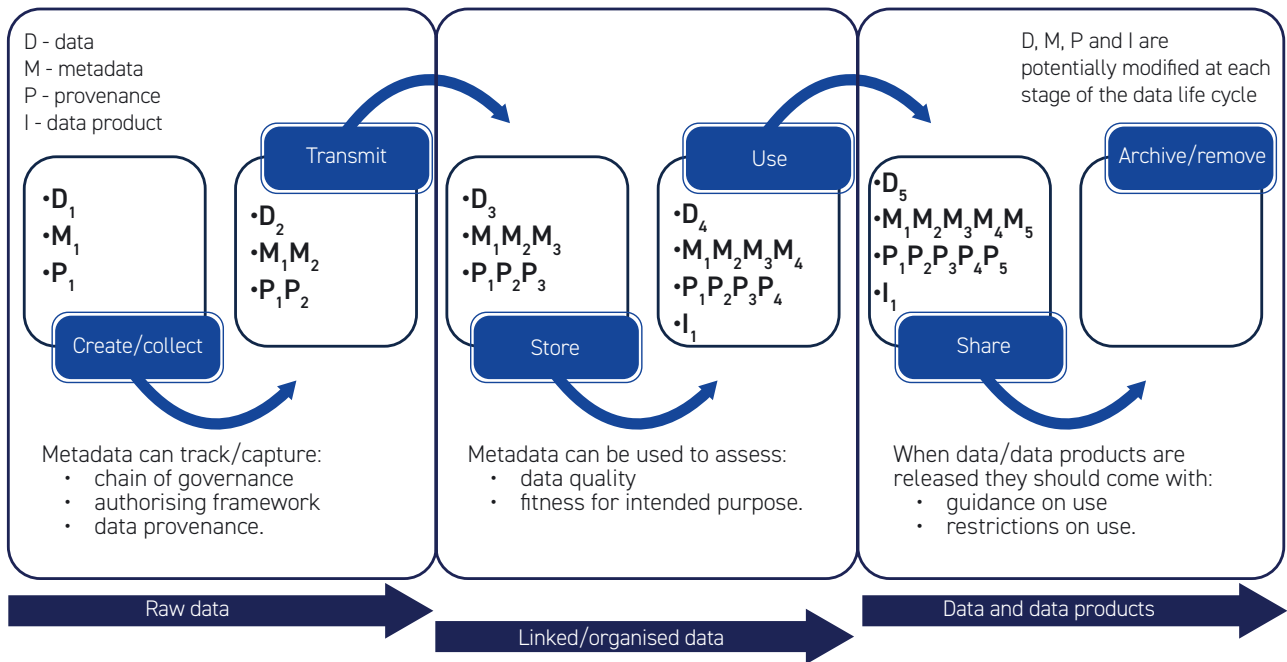


Figure 8: A simplified data life cycle

As data moves along the different stages of the life cycle, metadata can also be collected. Metadata ($M_1 \dots M_N$) can be collected that describes:

- data quality including accuracy, timeliness, completeness and consistency
- conditions under which data is collected/created, including context and environmental conditions
- data format: electronic data, paper-based data, data captured in other formats, and data encoding.

Special metadata ($P_1 \dots P_N$) on data provenance can be also collected, and it describes the journey of the data to the point of use, including:

- the authorising environment and regulations or policies under which data is captured, transmitted, stored, used and shared
- which entities have held the data
- which entities have accessed the data and for what purpose
- what transformations have been performed on the data.

Finally, as data is used for analysis, insights are generated (I_1), which can accompany the data for subsequent uses. Insights are a form of data product

derived from data and may have an independent life cycle from the data itself. Insights can be used, re-used or combined with other data or insights.

Focussing on access, use of and sharing/archival of data as the more general model, the considerations for data use become:

- an evaluation of the authority to access data/ insights/metadata based on an understanding of provenance data
- an evaluation of the appropriateness of the quality of data for the use intended
- an understanding of the format in which data will be accessed and used
- an evaluation of the authority to use data/ insights/metadata, based on an understanding of provenance data
- an evaluation of the authority to share data/ insights/metadata, based on an understanding of provenance data
- providing guidance on use of insights and data products created through updated metadata.

3.2 Ways of accessing data

Data sharing and use can involve more than taking a copy of data and using or analysing it without oversight. Different degrees of access can be provided, from none (most extreme), allowing access to prepared data products (including insights or aggregations), being able to run limited uses (such as queries), to providing a copy of the data without restriction. These concepts of access are shown in Figure 9.

These various modes of sharing and use require increasing levels of control, depending on the sensitivities associated with the data, or alternately, an assessment and reduction of the sensitivities of the data and data products.

The data products referred to are created from data. They can be aggregated versions, subsets of original data, perturbed data, an insight, chart, dashboard or any other result of use of data. Data products may have different levels of inherent sensitivity and different levels of personal information compared to the original data asset.

Limiting the use cases that a data requestor can apply to a dataset is a way to ensure that the context for the data is enforced through a 'requirement' for use. For example, if data about travel journeys were linked for an individual traveller over the course of a month, the ability gain fine-grained information about that user's movements is a risk for re-identification. A use case limitation may be that only two stages of any journey may be accessed in a query, limiting risk of identifying a unique traveller through a unique journey.

Similarly, if data products are created of pre-packaged 'insights', these can be assessed for privacy, sensitivity and quality issues before wider release. If privacy, sensitivity and quality issues are identified, then greater controls can be applied to the environment into which the data products are released and to the individuals who access them.

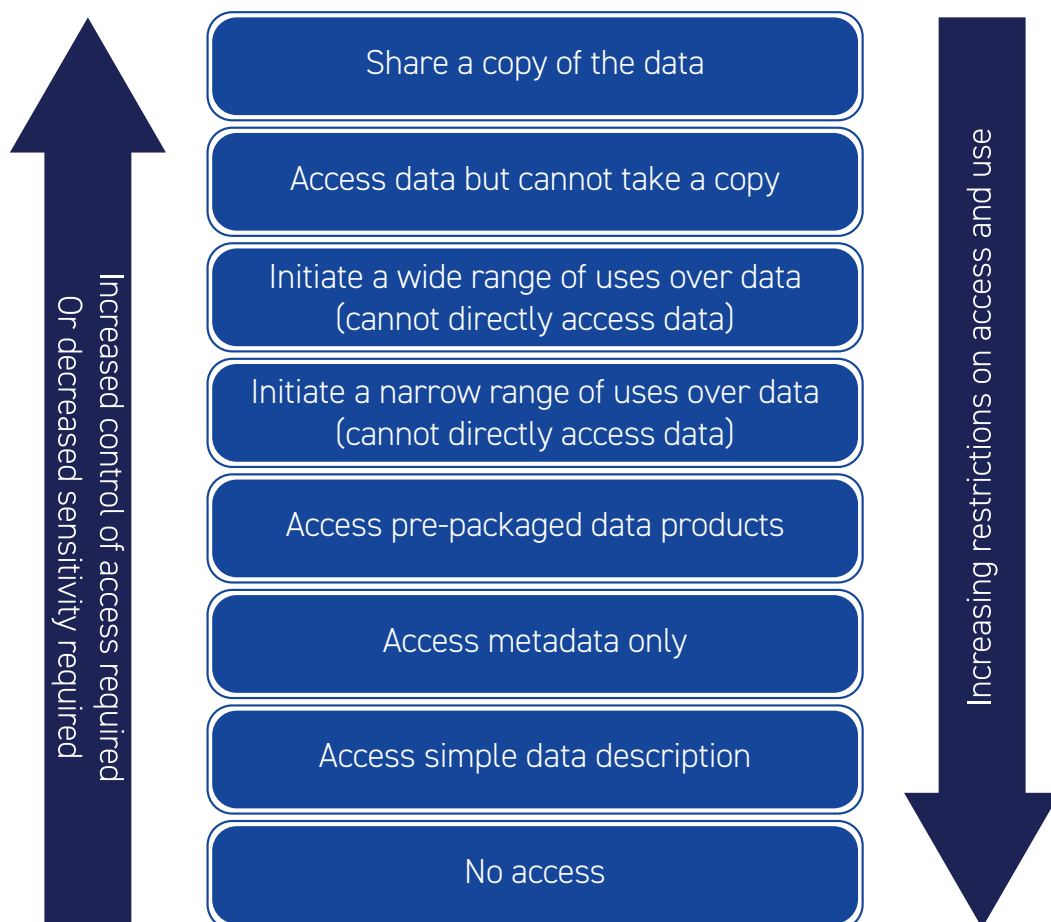


Figure 9: Framework for data sharing and use



3.3 Virtualisation anyone?

The creation of a dataset is the traditional framework for accessing data. By centralising data, it can then be accessed within appropriate controls for a wide range of purposes. The unintended consequences of creating a dataset, however, can be many, not least of which is giving access to potentially far more information that is required for the use cases intended, as well as potentially creating an attractive data asset for cybercriminals.

As potential data sources grow in number, size, complexity and geography, there are some 'megatrends' that are worth considering.

- Data is increasingly large and expensive to move. High refresh datasets may represent terabytes or petabytes of static equivalent data. The cost in time, money and energy to transfer the source may be prohibitive except in the most extreme cases.
- Data is of varying quality. The effort to improve data quality once extracted means the benefit is applied to the combined dataset rather than at the source.
- Data has varying levels of personal information and other sensitivities. As discussed earlier, combining multiple sensitivities may amplify the sensitive subjects in the source data.
- Data is bound by various restrictions on use. As discussed in the previous section, accessing the raw data itself may be prohibited.

- Data can quickly age and lose currency. A corollary of the data quality parameter of timeliness, 'old' data may quickly become irrelevant or at least only suitable for a narrow range of uses.

Unlike the traditional extract, transform and load (ETL) process, data virtualisation is an approach to data access and use that allows an application to retrieve and manipulate data without requiring its movement. The data remains in place, and real-time access is given to the source system for the data, still providing a single view of the overall data.

This approach reduces the risk of data errors, of the workload moving data around that may never be used, and it does not attempt to impose a single data model on the data. The technology can also support the writing of transaction data updates back to the source systems if this level of access is permitted. Abstraction and transformation techniques are used to resolve differences in source and consumer formats and semantics.

One important consideration of data virtualisation is that the connection to all necessary data sources must be reliable as there is no local copy of the data.

4. Considerations for using data

4.1 Who wants access to the data and why?

In surveys of data custodians and the general public, the intended use of the data has been frequently identified as a very significant factor when determining the risk framework for data sharing and use.

Ethics committees will often ask the 'why' question related to human research projects, but ethics committees are not used in all people-centred data projects.

A formal definition of 'data use' and 'use case' would bring clarity about what is intended for the data and what can be done with the results. Work is underway within standards bodies to try to formalise use cases for data (ISO/IEC JTC 1/SC 32/WG 6).⁹ Very often, however, a use case is described in terms of:

- who wants access to the data
- why they want to access the data
- consideration of the level of personal information in the data
- consideration of aspects of sensitivity of the data and the results of its analysis

- concerns about the level of granularity of access to the data
- concerns related to the use of insights and decisions generated from analysing data.

The sensitivity of any dataset relates to the level of personal information, the possible harms arising from the use of the data, and the concerns around unintended consequences of data availability.

Depending on the sensitivity of the data and how likely an individual is to being identified in the data, being able to explain 'who' and 'why' is becoming increasingly important. The safeguards required to be put in place also increase with sensitivity, levels of personal information being used and the risk of re-identification of individuals.

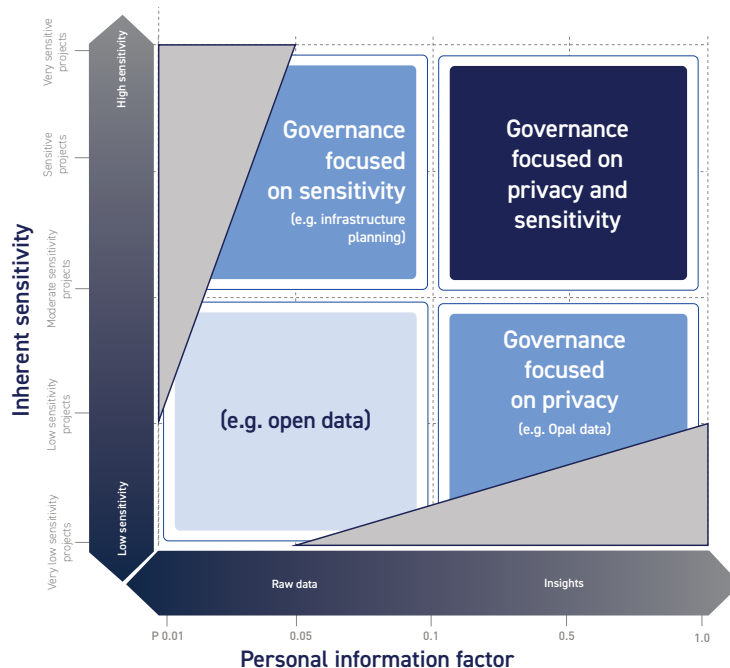


Figure 10: Simplified governance framework
Source: ACS (2021) Sharing data in trusted frameworks

⁹ See https://www.iec.ch/ords/f?p=103:7:512258326175321:::FSP_ORG_ID,FSP_LANG_ID:3406,25

4.2 Operational or non-operational

A useful way to frame the risks and considerations for use of data are associated with the division of application of data products created by 'operational' or 'non-operational' systems.

Operational data products are those created by systems that are expected to have a real-time (or near-term), real-world effect. The purpose is to generate an action, either prompting a human to act, or the system acting by itself. Operational data products include (and this list is not exhaustive):

- a monitoring signal – a human interpretable signal derived from a data source that may lead a person to act (for example, an ongoing temperature or humidity monitor)
- a prediction – a short term future forecast that may lead a person to act (for example, a weather forecast)
- an alert or alarm – a signal that is expected to draw the attention of a human (for example, a temperature warning light)
- a decision – a conclusion of analysis of data inputs (for example, a classifier deciding an object has been recognised)
- an action – an automated action, based on data input, which operates without human intervention (for example, an automated braking system).

Not all operational data-driven systems are high risk. An example of lower-risk operational data-driven system is the digital information boards that show the time of arrival of the next bus.

Operational data-driven systems that use real-time data to recommend or make a decision that adversely impacts a human are likely to be considered high or highest risk.

Non-operational data products are those created by systems that are not expected to have a real-time (or near-term), real-world effect. Rather, they may provide insight for consideration. A non-exhaustive list of non-operational data products includes:

- a simple analysis – an operation on a number of fields (for example, count, average, difference)
- a model – a re-usable framework derived from input data (for example, a digital filter)
- a modified data product – an aggregated or simply modified version of the input data that can subsequently be used (for example, data that has had selected fields removed or modified)
- an insight – a result (expected or unexpected) generated from input data (for example, a percentage of a population with a particular condition)
- a chart – a static representation of a system or environment (for example, a benchmark or a map)
- a dashboard – a non-real-time monitoring system with insights or charts.

Non-operational data-driven systems typically represent a lower level of potential risk. However, the risk level needs to be carefully and consciously determined, especially where there is a possibility that insights and outputs may be used to influence important future policy positions.

Operational data-driven systems are those that have a real-time (or near-term), real-world effect. The purpose is to generate an action, either prompting a human to act, or the system acting by itself.

Not all operational data-driven systems are high risk. An example of a lower-risk operational data-driven system is the digital information boards that show the time of arrival of the next bus.

Operational data-driven systems that use real-time data to recommend or make a decision that adversely impacts a human are likely to be considered high or highest risk.

Non-operational data-driven systems do not use a live environment for their source data. Most frequently, they produce analysis and insight.

Non-operational data-driven systems typically represent a lower level of risk. However, the risk level needs to be carefully and consciously determined, especially where there is a possibility that insights and outputs may be used to influence important future policy positions.



The risk profiles for use of operational and non-operational data products relates directly to their impact on the real world, the rate of that impact, the potential harms from that impact and mitigations that

are in place to limit any harms from those impacts. Figure 11 is adapted from NSW Artificial Intelligence Assurance Framework.¹⁰

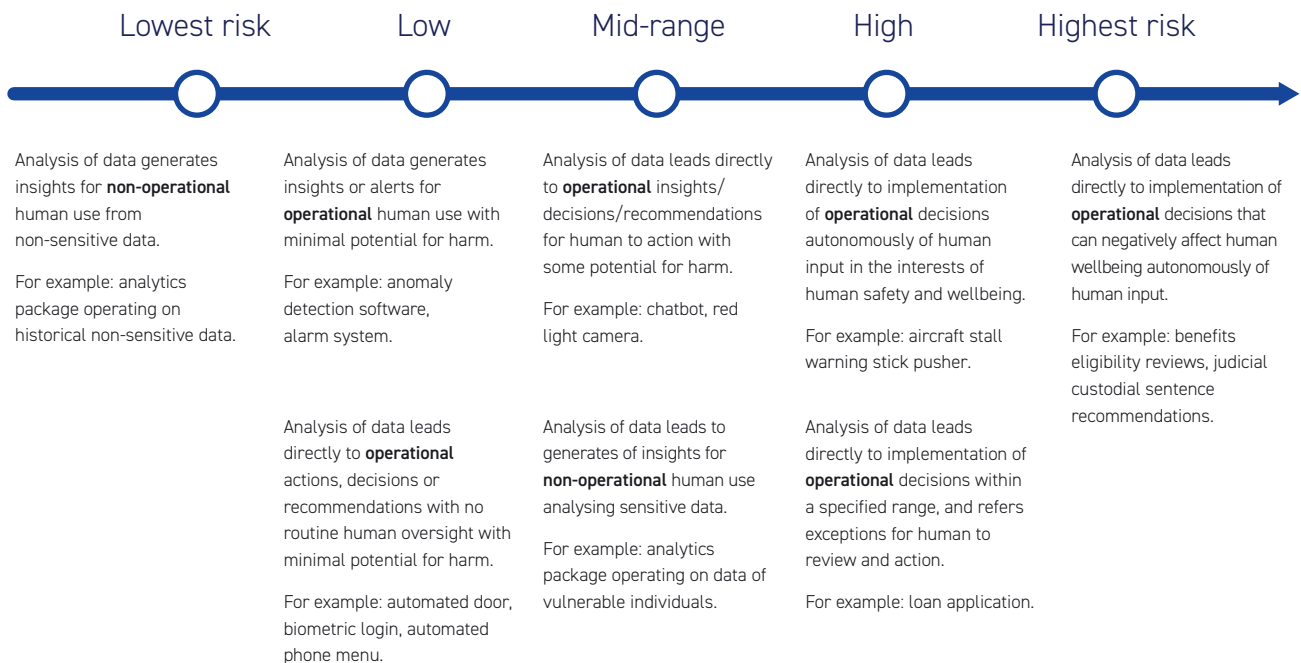


Figure 11: Risk profiles exist on a spectrum

Source: Adapted from NSW Government, NSW Artificial Intelligence Assurance Framework

¹⁰ NSW Government, NSW Artificial Intelligence Assurance Framework, <https://www.digital.nsw.gov.au/policy/artificial-intelligence/nsw-artificial-intelligence-assurance-framework>

4.3 Potential harms

The potential harms are largely driven by the real-world implications of application of a data product. Figure 12 shows a non-exhaustive list of harms associated with the use of data products and possible real-world adverse outcomes. The figure attempts to provide a scale to contextualise the potential harm in terms of how readily reversible that harm is. Figure 12 is adapted from the NSW Artificial Intelligence Assurance Framework.

An irreversible harm occurs when it is impossible to change back to a previous condition. An example is if a data-driven system makes an incorrect decision to deny somebody a pension without providing an option to have that overturned. It is important to consider how outcomes can be overturned in the event there is harm caused or the AI system leads to an incorrect decision.

In all real-world applications of data products, operational and non-operational, systems must be

closely monitored for harms that they may cause. This includes monitoring outputs and testing results to ensure there are no unintended consequences.

It is important to be able to quantify unintended consequences, secondary harms or benefits, and long-term impacts to the community, even when testing and during pilot phases of data-driven systems. Testing can still do real harm if the system is making consequential decisions. It is important to consider and account for this possibility even if human testers are willing volunteers.

Changing the context or environment in which the data products are used can lead to unintended consequences. Planned changes in how the data products are used should be carefully considered and monitoring undertaken.

Consider the risks of ...	None, negligible, N/A	Reversible with negligible consequences	Reversible with moderate consequences	Reversible with significant consequences	Significant or irreversible
Physical harms	○	○	○	○	○
Psychological harms	○	○	○	○	○
Environmental harms or harms to the broader community	○	○	○	○	○
Unauthorised use of health or sensitive personal information (SIP)	○	○	○	○	○
Impact on right, privilege or entitlement	○	○	○	○	○
Unintended identification or misidentification of an individual	○	○	○	○	○
Misapplication of a fine or penalty	○	○	○	○	○
Other financial or commercial impact	○	○	○	○	○
Inconvenience or delay	○	○	○	○	○
Other harms	○	○	○	○	○
	Very low risk or N/A	Low	Mid-range	High	Very high risk

Figure 12: Range of harms

Source: Adapted from NSW Government, NSW Artificial Intelligence Assurance Framework

4.4 Principles of fairness and the relationship to data

There are many issues which impact 'fairness' in the use of data products when applied to the real world. Services or decisions can impact different members of the relevant community in different ways. Whether due to cultural sensitivities, or underrepresentation in training datasets. It is important to think deeply about everyone who might be impacted by data-driven systems. Some of these are highlighted in Figure 13, which is also adapted from NSW Artificial Intelligence Assurance Framework.¹¹

Data quality is often described in terms of minimum requirements for accuracy, timeliness, completeness, and consistency. Data-driven systems may be significantly impacted by poor-quality data. It is important to understand how significant the impact is before relying on insights or decisions generated by the system.

Absence of data may lead to unintended biases impacting insights generated by data-driven systems. Unbalanced data is a common problem when training data-driven systems. It is also important to consider the impact with regard to gender and on minority groups, including how application of the data products created might impact different individuals in minority groups when developing the system. Minority groups may include:

- people with disability
- LGBTIQ+ communities
- people from CALD backgrounds
- Aboriginal and Torres Strait Islander peoples
- children and young people.

Consider the risks associated with ...	Very low risk or N/A	Low	Mid-range	High	Very high risk
Using incomplete or inaccurate data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Having poorly defined descriptions and indicators of 'fairness'	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Not ensuring ongoing monitoring of 'fairness indicators'	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Making decisions to exclude outlier data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Using informal or inconsistent data cleansing and repair protocols and processes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Using informal bias detection methods (best practice includes automated testing)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Re-running scenarios that could potentially produce different results (reproducibility)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Inadvertently creating new associations when linking data and/or metadata	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Having differences in the data used for training compared to the data for intended use	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Figure 13: Fairness principles

Source: Adapted from NSW Government, NSW Artificial Intelligence Assurance Framework

4.5 Prohibition, restrictions and guidance for use

After data products are created, it is important to provide frameworks around how the data products are to be used. The guidance can be in the form of:

- Prohibitions – absolute restrictions on how data products are to be used. Examples include legal prohibitions on data products being used by people outside of an authorising framework (for example, unauthorised access), or prohibiting use of data products for certain purposes (for example, law enforcement).
- Restrictions – enforced limitations on use of the dataset or data products. Examples may include

training requirements before an individual is allowed to access data products, or requirements for confidentiality limiting sharing of data products.

- Guidance – recommendations on how data products should be used. Examples include recommending that certain fields be used in conjunction with each other, or that certain fields not be used in particular circumstances. Not following the guidance should not lead to harms for those using the data products. If it could, the recommendations should be made as restrictions rather than guidance.



11 NSW Government, NSW Artificial Intelligence Assurance Framework, <https://www.digital.nsw.gov.au/policy/artificial-intelligence/nsw-artificial-intelligence-assurance-framework>

5. Bringing it all together

5.1 Application of controls based on risk – considerations and controls

This section provides an update of the governance frameworks described in the 2021 technical white paper *Sharing Data in Trusted Frameworks*.

In this section, we bring the respective pieces together and describe the ways to address the sensitivity versus privacy matrix through controls based on identified risk. After assessing a project for sensitivities, 'considerations' help to address these sensitivities and identify appropriate use of controls.

In the simplest of data life cycles, two entities may trust each other and establish protocols for data sharing and use with the characteristics discussed earlier in this paper. Once multiple stages of life cycle exist with data or data products on-sharing, more formal structures are required that allow confirmation of:

- authority to receive and use data
- authority to share data or data products
- confirmation of governance capability, systems and processes
- confirmation of technical capability
- confirmation of appropriate domain experience.

Figure 14 shows that some of these aspects interact to create 'very high control' environments, to 'no control' (or open) environments with no limitations on data sharing and use.

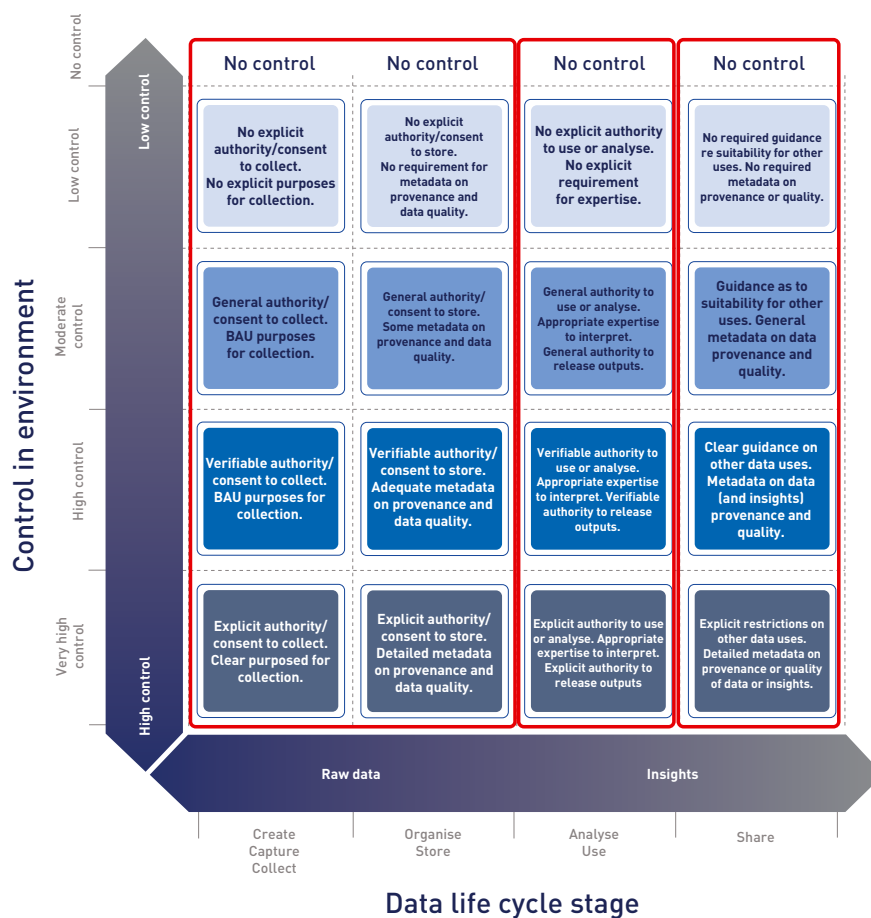


Figure 14: Characterising control layers for first stages in a simplified data life cycle

Control = (proven) capability * (assessable) governance * (verifiable) purpose

Capability includes skill in all stages of the data life cycle – data analysis, data provenance, governance and security.

High control = skilled people working in strong governance environment with clearly authorised purpose.

No control = no assessments or no restriction on people accessing or utilising data.

5.2 Characterising levels of control

Each of these controls requires an objective, repeatable, standardised assessment of:

- capability
- governance
- purpose
- data quality and provenance
- sensitivity of data
- degree of personal information contained in datasets.

These different control environments can be characterised as follows.

A **very high control** environment

must have:

- explicit purpose and authority to access and use data
- expert users experienced with the data of the quality provided and with associated metadata
- expert analytical capability and domain expertise
- strong governance and security at each stage of the life cycle
- explicit restrictions on release of data and insights, or secondary use of data and insights
- people who have met general expertise requirements as well as project-specific requirements for a 'Safe Person' and agree to be bound by limitations on data access and use.

is suitable for:

- data that can only be accessed under an external instrument such as a public interest disclosure (PID)
- data that is reasonably personally identifiable
- data that contains sensitive subject matter
- data that has a well-quantified quality.

A **high control** environment

must have:

- explicit purpose and authority to access and use data (although it may not have project-specific requirements)
- expert users experienced with the data of the quality provided and with associated metadata

- very skilled analytical capability and domain expertise
- strong governance and security at each stage of the life cycle
- explicit restrictions on release of data and insights, or secondary use of data and insights
- access restricted to people who have met general expertise requirements for a 'Safe Person' and agree to be bound by limitations on data access and use.

is suitable for:

- data that is not reasonably personally identifiable
- data that contains sensitive subject matter
- data that has a well-quantified quality.

A **moderate control** environment

must have:

- general purpose and authority to access and use data (such as an authorising regulatory framework)
- experienced users dealing with the data of quality provided and with associated metadata
- skilled analytical capability and domain expertise
- strong governance and security at each stage of the life cycle
- general restrictions on release of data and insights, or secondary use of data and insights
- access restricted to people who have met general requirements for a 'Safe Person' and agree to general conditions on data access and use.

is suitable for:

- data that is not reasonably personally identifiable
- data that contains some sensitive subject matter
- data that is of sufficiently high quality for the intended use.

A **low control** environment

may have:

- no explicit authority to collect and use data, but no known restrictions to use data
- users with some experience dealing with data of the quality provided

- users with some analytical capability and domain expertise
- appropriate governance and security at each stage of the life cycle
- may not have restrictions on release of data and insights, or secondary use of data and insights.

is suitable for:

- data that is not reasonably personally identifiable
- data does not contain sensitive subject matter

- data that is of sufficiently high quality for general use.

A **no control** environment

may have:

- no controls in place.

is suitable for:

- data that has been approved for release as open data
- data that is of sufficiently high quality for general use.

5.3 Determining the level of control required

The question to ask now is: what level of control do I require for data sharing and use?
Taking the characteristics of the different control

environments in reverse order, a series of questions can be asked to help identify the level of control required.

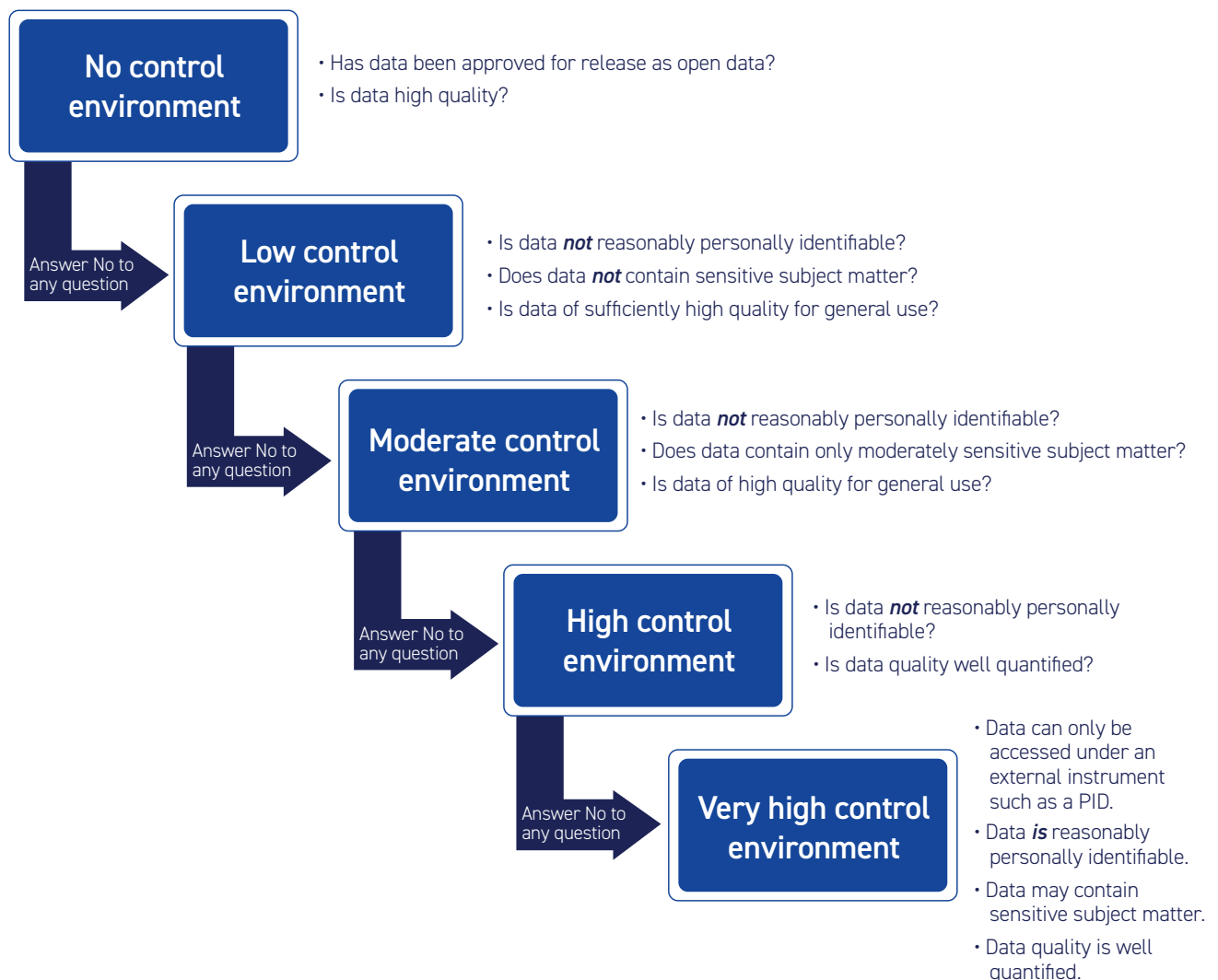


Figure 15: Level of control required for data sharing

5.4 What about people?

The control model has an element of people with technical, domain and governance experience. The general requirements for a person to work on a project include that they:

- are verifiably skilled and experienced in their domain's techniques – for example, an analytical expert, governance expert or cyber expert
- have been screened or endorsed by independent authorities – for example, someone who has been endorsed by an executive manager or has completed a police check or working with children check
- understand and agree to be bound by legal frameworks such as privacy protection legislation and health record protection legislation
- understand and agree to follow formal governance processes used in the analytical environment
- understand the roles of others in the analytical chain and governance process, and agree to respect and work with these roles
- understand and are able to use the specific tools and processes in the analytical environment.

From a project-specific standpoint, they:

- are expressly authorised to work with the subject data for an authorised project
- understand and agree to be bound by project legal agreements or restrictions such as a public interest disclosure (PID) or other project-specific restrictions.

Individual privacy considerations

As discussed earlier, the knowledge held by a person viewing a dataset or insight may lead to re-identification. Understanding the connection an individual has to a dataset could be an additional consideration.

Additional measures for a person accessing data may include the following elements:

- personal connection to the dataset – understanding the degree of separation between the people represented in the dataset, or the region represented, and the analyst
- accountability – the personal consequences for the analyst in the event that re-identification does occur (PII is attained), PII is released or that PII is used inappropriately by the analyst.

Figure 16 shows the different roles of Safe Persons in the analysis/use phase of the data life cycle.

The different roles in the analysis phase include identifying:

- someone with the authority to receive the data and bring it into the analysis phase
- someone with security/governance responsibility
- someone with the required analytical skill at the level of expertise required by the level of the control environment
- someone with domain expertise
- someone with delegated authority to release data and insights, along with restrictions on use and secondary use.

In practice, several of these roles may be held by one person. The roles highlighted in orange are those that may have project-specific requirements, depending on the level of control of the environment. The other roles are generic for any project involving people-centric data.

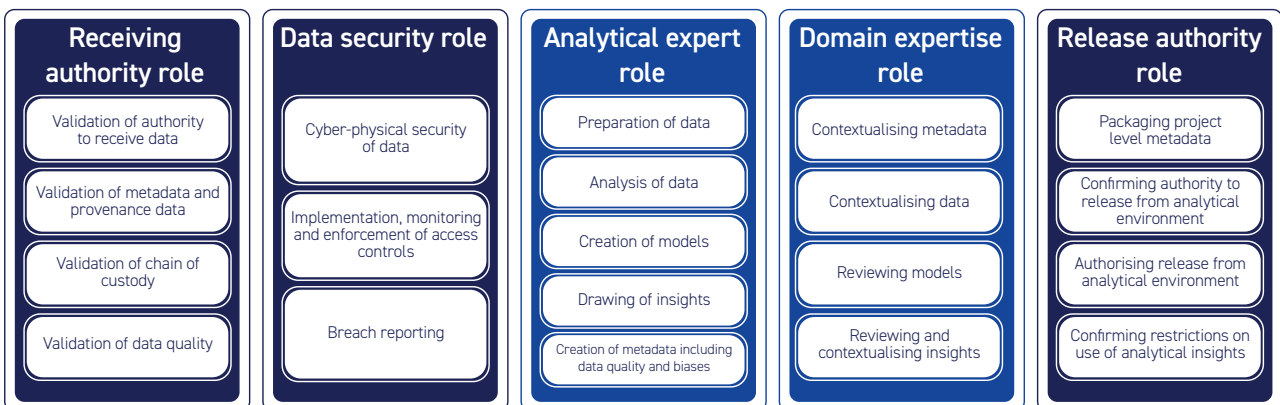


Figure 16: Roles in the analyse/use stage

5.5 Moving between layers of control

An important point to note is that 'use' of data can create data products with lower (or higher) levels of control. One obvious way of creating a data product is the through aggregation or perturbation of raw data values. The data product created should meet predetermined thresholds for minimum identifiable cohort size (see the discussion of MICS in Section 2.5).

It is also possible to create a data product that requires a higher level of control if it is shared with an entity that has the ability to link additional data to the product created, or has additional context not known to the

users involved in creating a data product under a particular level of control.

An example is an analytics team operating on a de-identified dataset to produce a set of insights. If these insights are then provided to a client agency that has additional information as to individuals known to be in the dataset, and with the ability to identify individuals must treat operate with the insights within a greater level of control that the team who produced the de-identified insights.

Data controls in use: An example

Consider an example of a transport organisation that collects and uses real-time data of bus location and estimated loading to improve fleet performance in real time. The dataset is also used by the organisation to create an open-source data product for developers to build mobile applications to track approximate bus location in real time.

Considerations for use of the data

Bus locations are not considered sensitive if less accurate than a predetermined spatial limit. The real-time location details are intended to support use cases internally within the organisation, including:

- locating a bus on its current route
- predicting bus arrival times
- estimating how full a bus is and if more capacity is required
- predicting next-best-bus-options and modal interchange options for potential passengers
- predicting if additional bus services are needed.

Lower (spatial) resolution versions of the real-time data asset are intended to support use cases by app developers and public users outside of the organisation, including:

- approximating the location of a bus on its current route
- estimating approximate bus arrival times
- indicating the likelihood of getting a seat on the bus.

Two data products are to be produced and managed – within a 'moderate control' environment for internal use within the organisation by employees (bound by confidentiality agreements) and within a 'no control' environment for use by people external to the organisation.

Restrictions on use

Access to high-precision bus latitude and longitude must only be provided to people within the transport organisation who have formally committed to treat the information in a confidential manner. Bus latitude and longitude must be perturbed to a pre-agreed level for the no control environment. Access to bus loading levels must only be accessed within the organisation. Predetermined thresholds (for example, light, medium, heavy) are provided to users outside the organisation.

Guidance on use

Detailed technical guidance on use of bus latitude and longitude is provided to the organisation's internal developers. Technical guidance on how to interpret bus latitude and longitude is provided for external users.

Quality requirements

Fields should not be blank unless BLANK is a valid option. Entries in the dataset should match the expected field type (for example, integer, Boolean, string, floating point). Bus latitude and longitude and estimated bus loading should be validated at the bus depot at the start and end of every unique bus shift.

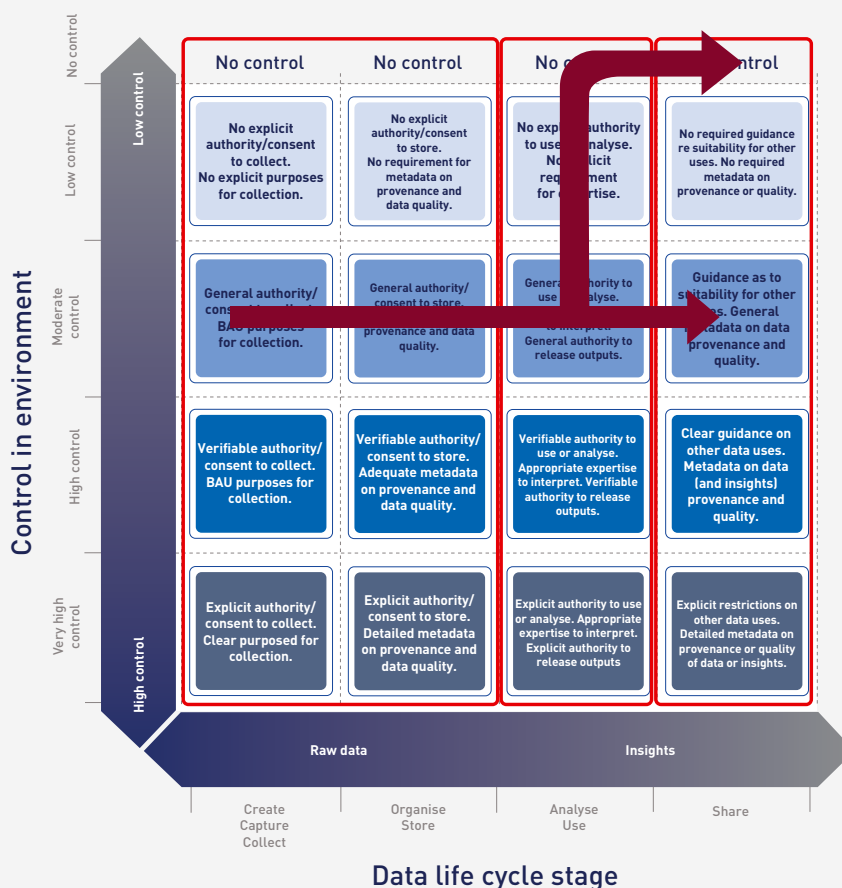


Figure 17: Example of data products created with different levels of control

Two data products which could be created are:

- No control environment: Raw data without personal information and with perturbed location information made publicly available.
- Moderate control environment: Raw data with accurate location information. Accessed by planners and policy makers operating within transport organisation rules and appropriate regulations.

A high control environment is not required as data collection and use does not contain personally identifiable information.

A very high control environment is not required as data collection and use does not require a special legal instrument.



6. Discussion

The work presented in this paper is an ongoing effort to identify frameworks to safely share and use data. The work identifies controls required to ensure that data is treated appropriately along the entire data life cycle. It is this, often unknown, life cycle that creates so much concern for data custodians and others involved in the data ecosystem, including data subjects themselves.

6.1 The work on PIF is continuing – OptimShare

The PIF as described in the 2019 ACS technical white paper *Privacy-Preserving Data Sharing Frameworks* was a first attempt at defining this parameter and creating a practical tool. The PIF uses information theory to compute privacy risk in a dataset. The tool suggests the associated risks and proposes recommendations for sharing data, for example, suppression of certain attributes. The analysis results are also displayed as visuals, which makes interpretation easier. Based on the associated risks, the tool uses a provable privacy technique (for example, differential privacy) to perturb data.

The Cyber Security CRC, led by CSIRO's Data61, has continued to develop the original PIF tool and build it into data sharing frameworks. Unlike traditional tools that choose design parameters in an ad hoc fashion, the new AI-based framework considers various attack vectors, user risk appetite and the required level of accuracy to select the design parameters (see Figure 18 below).

The evolved PIF Tool (OptimShare) assesses privacy risk in a dataset and provides recommendations while publishing or sharing data. The AI-enabled framework automatically transforms the data to mitigate the identified risks (where possible) using provable privacy techniques such as differential privacy.

Previous approaches to solving this problem provided an algorithmic solution that concentrates on modifying a dataset to obtain a privacy-preserving version. These algorithmic solutions do not provide a robust risk analysis of the input data before being modified for release.

Different algorithms tend to apply an extreme level of randomisation that leads to unusable data.

While there are a few framework-based privacy evaluation solutions, none of these approaches successfully balances data privacy and utility.

The new tool provides a unified privacy-preserving framework that effectively balances the privacy and utility of tabular data sharing.

OptimShare first evaluates the risk of personal information disclosure linked with a particular tabular dataset. This is done through an information-theoretic approach by evaluating the PIF.

The PIF provides an interactive way to identify the risk landscapes of input data. It determines different types and levels of risks to assess the overall risk of releasing a dataset.

Someone who aims at exploiting data is able to narrow down rows that could potentially reveal individuals' personal information. By looking at what an attacker would be most interested in, it is possible to distinguish between field and table risks ranging from a low-risk to a high-risk level. Then, an AI-enabled engine conducts privacy preservation of the tabular data according to the risks identified through a list of advanced techniques based on information theory, fuzzy logic and differential privacy.

Through a fuzzy inference engine, OptimShare enhances the privacy requirements of the underlying dataset. An iterative process is then carried out to systematically apply privacy-preserving data generation with identified privacy appetite, satisfying differential privacy.

Next, the generated data is rigorously assessed through an iterative process for performance against target applications before release. This results in a privacy-preserving tabular dataset that can maintain both strong privacy and utility.

The PIF-based analytical framework of OptimShare is available as open source.¹²

¹² <https://github.com/PIFtools/piflib>

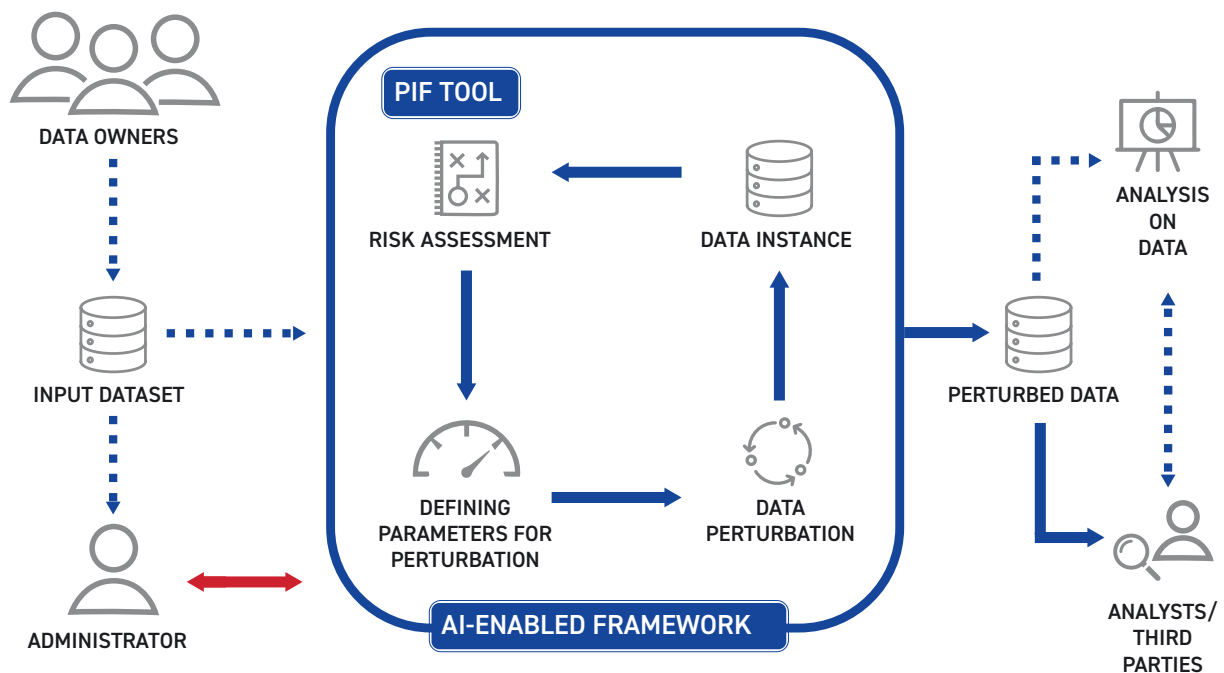


Figure 18: Overview of ongoing work to evolve the PIF

Source: Data61

6.2 Advances in data and digital standards

Standards are fundamental to systematic data sharing. Standards on terminology, use cases, ways of sharing, roles, and responsibilities as well as governance and security are all important elements to ensure safe data sharing and use. There is a great deal of work taking place in the world of standards, which provides useful resources for data sharing frameworks. Standards Australia is the national member body at ISO¹³ and the IEC,¹⁴ as well as JTC 1, its joint technical committee focused on intersectional information technology.

The most relevant groups within the IEC/ISO JTC 1 family include subcommittees (SC) for data sharing and use include:

- SC 27 – Information security, cybersecurity and privacy protection
- SC 32 – Data management and interchange
 - within SC 32, Working Group 6 (WG 6) on data usage
- SC 38 – Cloud computing and distributed platforms
- SC 40 – IT service management and IT governance
- SC 41 – Internet of things and digital twin
- SC 42 – Artificial intelligence.

Australia is a participating member in eight data and digital standards committees at the international level, and Standards Australia convenes national 'mirror' committees correlating to each. Members of these national committees influence standards development in the international committees they mirror, by casting an Australian vote and in some cases by actively participating in international meetings. They also work on identical or modified adoptions of international standards, and on national standards as deemed necessary.

As of July 2022, Australia has adopted 26 international standards as Australian Standards from the 248 international publications since 2016.

Nine of these relate to smart cities, another nine relate to information and cyber security, and eight to Internet of Things and related technologies. There are further adoptions currently in the pipeline in the fields of artificial intelligence, cyber security and smart cities.

13 International Organization for Standardization <https://www.iso.org/home.html>

14 International Electrotechnical Commission <https://www.iec.ch/homepage>

Title	International committee	Australian mirror committee
Artificial intelligence	ISO/IEC JTC 1/SC 42	IT-043
Data management and interchange	ISO/IEC JTC 1/SC 32	IT-027
Information security, cybersecurity and privacy protection	ISO/IEC JTC 1/SC 27	IT-012
Internet of things and digital twin	ISO/IEC SC 41	IT-042
Cloud computing	ISO/IEC JTC 1/SC 38	IT-038
Electrotechnical aspects of smart cities	IEC SyC smart cities Electrotechnical aspects of smart cities	IT-269
Sustainable cities and communities	ISO/TC 268	IT-268
Smart cities	ISO/IEC JTC 1/WG 11	JT-001-11 WG 11

Figure 19: International committees and Australian mirror committees

Source: Standards Australia (July 2022) *Data and Digital Standards Landscape*

Title	International publications	Nationally adopted
Artificial intelligence	9	1
Data management and interchange	39	0
Information security, cybersecurity and privacy protection	138	9
Internet of things and digital twin	24	8
Cloud computing	18	1
Smart cities	40	9
	268	28

Figure 20: Documents published and nationally adopted, 2016 to 2021

Source: Standards Australia (July 2022) *Data and Digital Standards Landscape*

7. Conclusions

Many people have tried to find an analogy for data to help us think through what we have, how we can safely use it and what we need to harness its power. Analogies of 'data is the new' oil/asbestos/water all have some merit but miss a number of fundamental characteristics of data. A dataset may be relatively benign, but joined with another dataset, it may suddenly change. Data can be used and re-used without impacting its quality. Data can be shared infinitely and used differently each time.

A reasonable analogy for data is electricity. It took us more than 100 years to develop ways of safely handling electricity of different voltages and currents, but now electricity is literally everywhere in our lives, from lighting to vehicles, from computers to digital watches. We need to develop safe frameworks to work with the equivalent of 240 V data as well as 24,000 V data.

The frameworks presented here are a part of that work. They provide a working, if not fully complete, model for how to reduce the risks associated with the sharing of data while still enabling the benefits. Combined with the four previous ACS white papers, we hope they can provide a workable foundation for business and government to enable the sharing of data with confidence, and thereby reap the benefits that shared data can deliver.



8. Thanks

This paper was the culmination of more than six years' work by a Taskforce that included ACS, the NSW Data Analytics Centre (DAC), Standards Australia, the office of the NSW Privacy Commissioner, the office of the NSW Information Commissioner, the Australian Government's Digital Transformation Agency (DTA), CSIRO, Data61, the Department of Prime Minister and Cabinet, the Australian Institute of Health and Welfare (AIHW), SA-NT DataLink, the South Australian Government, the Victorian Government, the Western Australian Government, the Queensland Government, the Communications Alliance, the Internet of Things Alliance Australia, Ambiata, Data Synergies, Creator Tech, Objective, EY, Microsoft, Clayton Utz and several other companies.

Thanks go to the contributors to many, many workshops over six years, including:

Lyria Bennett Moses, Kimberlee Weatherall, Stephen Hardy, Peter Leonard, Chris Radbone, Geof Heydon, Sonya Sherman, Mathew Baldwin, Geoff Neideck, Frank Zeichner, Malcolm Crompton, Geoff Clarke, Kate Cummings, Ghislaine Entwisle, Ghazi Ahamat, Ben Hogan, Scott Nelson, Adrian Watson, Rachael Fraher, Alex Harrington, Andy West, Angelica Paul, Ashton Mills, Brian Thorne, Bridget Browne,

Cassandra Gligora, Chris Mendes, Daniel Marlay, Dominic Guinane, Kelda McBain, Liz Bolzan, Luke Giles, Marilyn Chilvers, Matthew Roberts, Matthew McLean, Michael Wright, Mike Willett, Peter Hatzidimitriou, Rick Macourt, Robin van den Honert, Roulla Yiacoumi, Shona Watson, Suyash Dwivedi and Tiffany Roos.

And finally, thanks to all others who have made, and continue to make, contributions and feedback.



9. Appendix – building a dataset in action

This appendix describes considerations for the development of a dataset of automated external defibrillators (AEDs) in NSW, with the goal to ensure the quality of the dataset is as high as possible at all times and provide access to a wide range of users.

Note: The description in this appendix is an example of how to address the considerations and challenges of creating such a dataset rather than a description of a process that occurred in practice.

Project scope

The scope of the project is to:

- identify a minimum feature set relevant to defibrillator location and condition in NSW (location, availability, type, functionality, condition, previous use, malfunctions)
- develop a systematic way of capturing the minimum feature set from deployed defibrillators in NSW to create the statewide dataset
- develop a systematic way to add, remove or update the dataset as the deployed defibrillator network changes over time
- develop a systematic way to reliably access and query the dataset.

In order to:

- identify and maintain an accurate dataset reflecting the current state of the defibrillator network in NSW
- provide reliable widescale public access to the dataset
- provide appropriate guidance on use of the dataset.

The project does not explore:

- developing applications using the dataset (example applications may be used to help refine requirements of the dataset or access requirements for the asset)
- developing proposals which impact emergency services operations
- developing recommendations for future deployment of defibrillators
- medical aspects of defibrillation (including use of patient data)
- economic aspects of defibrillator utilisation
- social aspects of defibrillation (bystander willingness to use defibrillators).

Example use cases

The AED dataset is expected to facilitate a number of use cases. For illustrative purposes, these are highlighted:

- **First responder application.** In the event of an out of hospital cardiac arrest (OHCA), a mobile application may show the location of publicly accessible AEDs in the vicinity of the victim of the OHCA. This use case requires real-time access to location, accessibility, and operational condition of the AEDs in the vicinity of the OHCA. This use case should not have access to personal information or information about AEDs in restricted areas.
- **Coverage mapping.** Someone planning the location of new AEDs may seek to understand the spatial distribution of publicly available AEDs at different times of the day or days of the week. This use case requires non-real-time access to AED location, accessibility times and operational condition of publicly available AEDs across NSW. This use case should not have access to personal information or information about AEDs in restricted areas.
- **Research.** A researcher may seek to understand the propensity of private ownership of AED. This use case requires non-real-time access to location of all AEDs across NSW both public and private. The researcher should be bound by appropriate restrictions if accessing information about AEDs in restricted areas.
- **AED maintenance.** A NSW government data custodian may seek to periodically update AED information in the dataset. This will require them to access personal information in the form of contact details of people responsible for AEDs. The data custodian should treat personal and sensitive information in accordance with NSW legislation and the consent received from the person responsible for the AED.

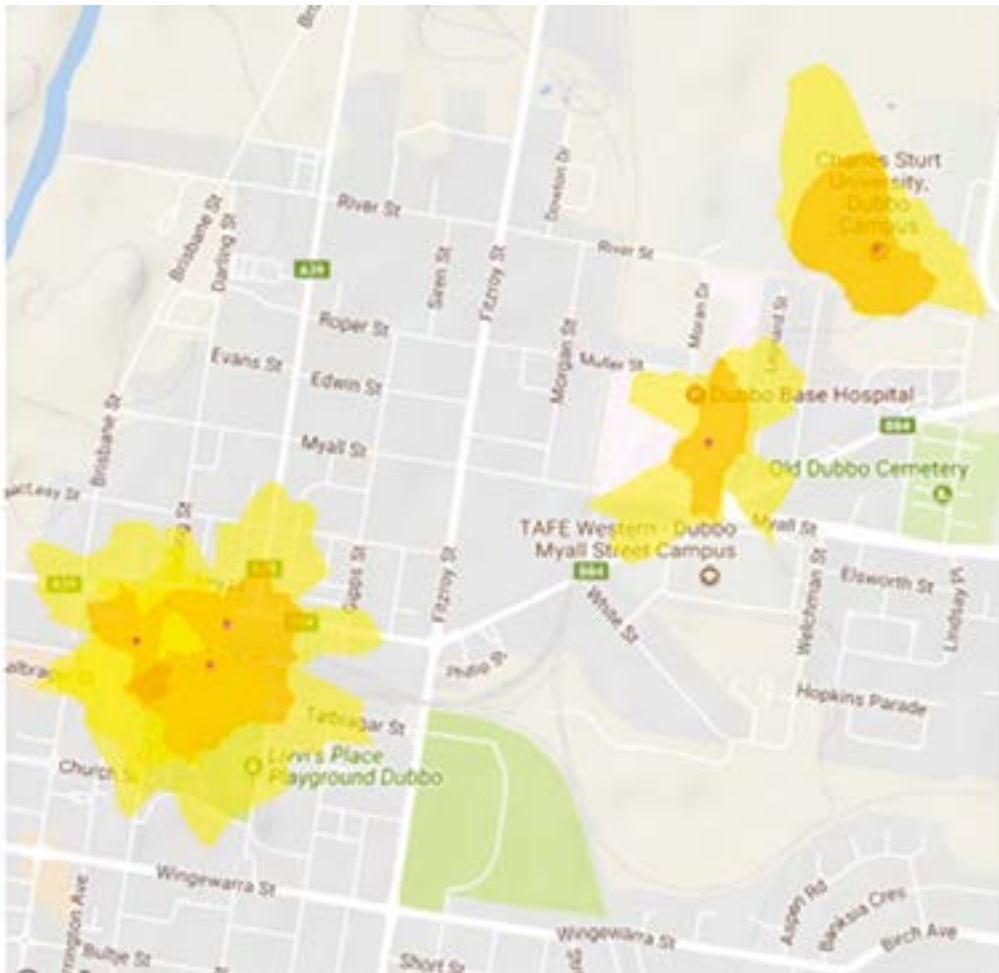


Figure 21: Example AED coverage map

Relevant policies and standards

The AED Dataset meets the criteria for a spatial dataset within the appropriate NSW data policy. Once collected, the AED Dataset will require the creation of appropriate metadata fields. This metadata will be required to be maintained along with the AED Dataset itself.

The preparation of metadata for a spatial dataset is the responsibility of the producer of the dataset. Custodian agencies should ensure the producer of the dataset is informed about this responsibility and ensure that the metadata is Australian New Zealand Land Information Council (ANZLIC) compliant.

Metadata shall be recorded for all datasets subject to these guidelines and the metadata shall be made freely available at no cost. The metadata statements must adhere to the NSW Guide to Metadata Creation (2012).

Custodians should use the following:

- NSW Metadata Element Set User Guidelines for Vector Datasets

- ANZLIC Metadata Profile Guidelines version 1.2 and the ANZLIC Metadata Profile.

Custodians should:

- Provide new and updated metadata records to the NSW Spatial Data Catalogue as soon as possible after the creation of a dataset, and in accordance with the NSW Guide to Metadata Creation. The NSW Spatial Data Catalogue is the accepted register in which all metadata for NSW spatial data should be lodged.
- Establish documented processes and procedures for the creation, management, and use of metadata. Copies of the NSW Guide to Metadata Creation (2012) and NSW Metadata Element Set User Guidelines for Vector Datasets are available from the NSW Spatial Data Catalogue.

Privacy and personal information considerations

Custodian agencies are responsible for ensuring that access to spatial data does not compromise privacy and personal information rights of affected parties. Adherence should be given to the *Government Information (Public Access) Act 2009* (NSW) and the *Privacy and Personal Information Protection Act 1998* (NSW) (PIIP Act) prior to the release of spatial data.

Custodians should consider the following questions:

- Does the spatial data contain personal information as per the PPIP Act or the *Health Records and Information Privacy Act 2002* (NSW)?
- Does the spatial data contain confidential information?
- Is there an overriding public interest against disclosure that would prevent this spatial data being released?

Mandatory metadata requirements

The NSW Spatial Metadata Policy recommends all state government agencies and local government authorities provide metadata for corporately significant spatial data they produce or enhance, or that is exchanged between agencies, and they should make this metadata publicly accessible via the NSW Spatial Data Catalogue.¹⁵ Figures 22 and 23 depict the decision framework in spatial metadata creation in NSW.

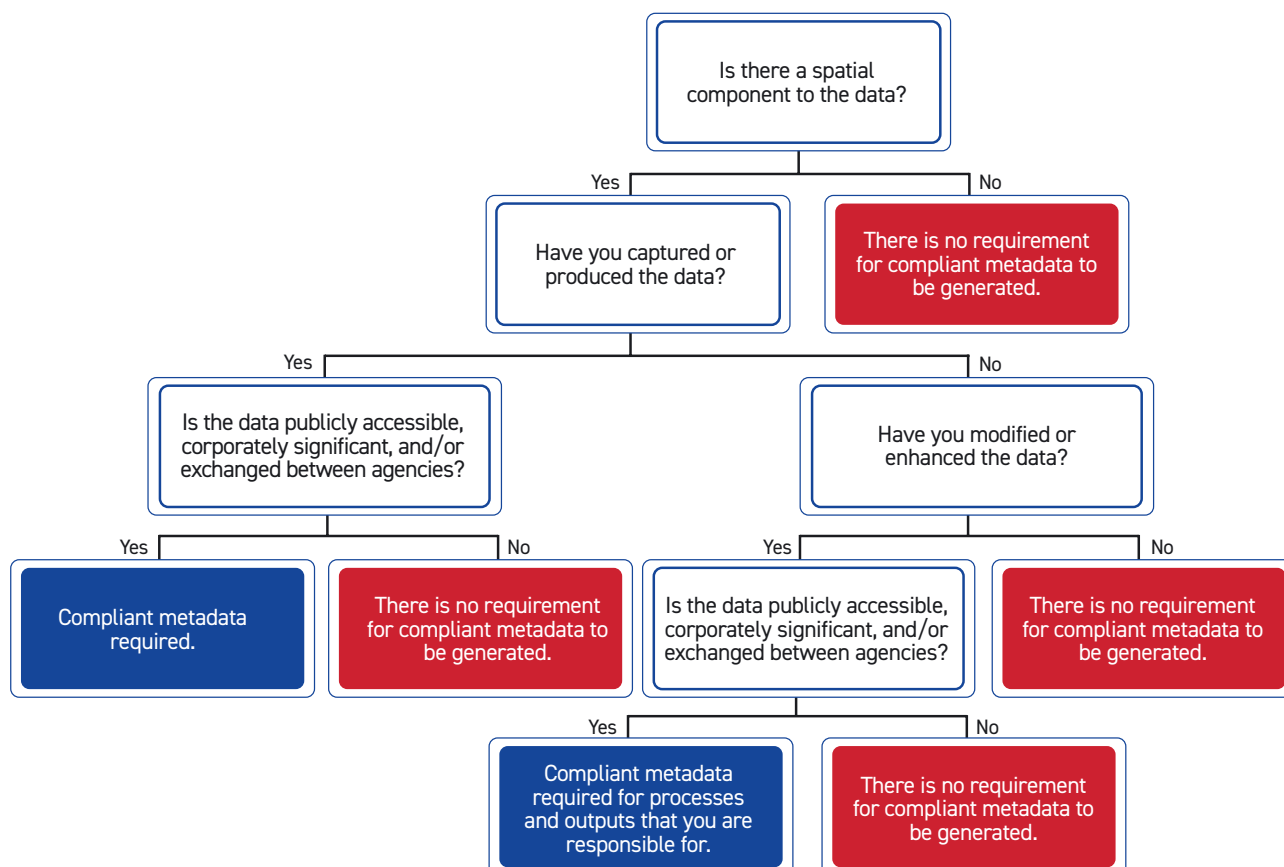


Figure 22: Decision matrix for the creation of spatial metadata

Source: NSW Government Land and Property Information (2012) *NSW Spatial Metadata Program*, NSW Spatial Services

15 https://www.spatial.nsw.gov.au/_data/assets/pdf_file/0017/190511/Metadata_brochure.pdf

Minimum elements for metadata in NSW	Description
Title	The name of the data layer.
Abstract	Similar to an executive summary.
Purpose	Why the data was created and what it was meant to achieve.
Metadata contact organisation	Organisation contact details for the metadata content.
Geographic location – coordinates	The spatial extent of the data: east/west longitude and north/south latitude.
Lineage	From what other data was this data constructed and what methods were used to create the dataset?
Temporal extent	Over what period was the data captured?
Distribution format	The data file format, web map service, etc: <ul style="list-style-type: none"> • name • version.
Keywords	Words that can be used in a search to find metadata record.
Maintenance frequency	How often is the data updated or maintained?
Use limitation	What are the constraints and limitations on how the data can be used?
Legal restrictions	Copyright and intellectual property permissions: access and/or use.

Figure 23: Metadata fields that are mandatory in NSW

Source: NSW Government Land and Property Information (2012) *NSW Spatial Metadata Program*, NSW Spatial Services.

Data management plan

Custodians must be aware that spatial data is a long-term asset of the state, and so access arrangements must be managed to support ongoing data access into the future. Data management plans may also need to reflect existing national frameworks when defining business needs for spatial datasets. A record of the dataset prior to changes or updates taking effect should be made in order to preserve the legacy of the dataset.

A data management plan assists in the management of a custodian agency dataset over the data life cycle, recognising the roles and responsibilities required to manage a particular dataset.

Publishing

Custodian agencies must ensure metadata is freely available to all discoverable, accessible and current data. They are responsible for the publication of the following:

- ANZLIC-compliant metadata
- NSW Spatial Dataset Profile(s).

Metadata can be published using an online metadata entry tool or using the ANZMet Lite tool, enabling ANZLIC-compliant metadata to be exported. The NSW Spatial Dataset Profile should be completed by the custodian agency of a spatial dataset for publication on the NSW Spatial Data Catalogue.

The discoverability of the dataset via large search engine sites should be a consideration of the custodian agency. As the AED Dataset would contain both personal information and information about AEDs in restricted (non-publicly available) areas, care should be taken as to when these fields are released. For example, personal information or information about AEDs in restricted areas should only be released with consent of the AED owner and with appropriate confidentiality undertakings from the recipient.

AED data features

The minimum dataset is intended to capture details of responsible AED operators and owners, AED locations and helpful guidance to access AEDs, AED accessibility information, and AED operational information.

It does not reflect AEDs that are mobile (such as with police or ambulances) but does provide the capability of both AED owner fields and crowdsourced information to be included in the AED Dataset.

Minimum data features

These features represent a minimum dataset can be used to locate an AED and to identify the responsible person from whom more information can be sought.

AED ownership and contact details

The information provided in these fields are for the primary contact and alternate contact for AEDs. The contact details are intended to support uses including:

- contact by NSW data custodian for data quality verification
- contact by NSW data custodian for data update
- AED location/availability/condition alerts
- AED maintenance alerts.

Private owners of AEDs may validly not have an organisation AED_OWNER_ORGANISATION_NAME.

Restrictions on use: The fields containing personal information should be treated according to the NSW *Privacy and Personal Information Protection Act (1998)*.

Guidance on use: These contact details should not be used for latency-sensitive operations.

Quality requirements: Fields should not be blank unless explicitly included as a valid option. Fields should match Field Type. CONTACT_POSTAL_ADDRESS should be compliant with Australia Post standards.

Details of contact person and organisation	Field Description and Type	Example	Sensitivity
AED_OWNER_ORGANISATION_NAME	Description: Name of the organisation that owns the AED. String: A free text name of a business or organisation. May be 0 to [255] characters.	Cobar Cricket Club	May validly be blank. Not recommended for use during latency-sensitive operations.
AED_CONTACT_PERSON_NAME	Description: Name of the person responsible for AED data/maintenance. String: A full name of a person, which can include first names, middle names or initials, and last names. May be [2] to [255] characters.	Jane Doe	Treatment of personal information must be compliant with appropriate legislation and policy. Must be validated before including the AED in the dataset.
CONTACT_PHONE_NUMBER	Description: Phone number of AED_CONTACT_PERSON_NAME. Telephone number: ACMA-compliant format.	0400 123 456	Treatment of personal information must be compliant with appropriate legislation and policy. Must be validated before including the AED in the dataset.

CONTACT_EMAIL_ADDRESS	<p>Description: Email address of AED_CONTACT_PERSON_NAME.</p> <p>Email address: The maximum length of the domain name is 255 characters, and the maximum length of the local part is 64 characters.</p>	JDoe from ccc.org.au	<p>Treatment of personal information must be compliant with appropriate legislation and policy.</p> <p>Must be validated before including the AED in the dataset.</p>
CONTACT_POSTAL_ADDRESS	<p>Description: Postal address of AED_CONTACT_PERSON_NAME. May be different to the AED location.</p> <p>String: Compliant with Australian Post standards.</p>	PO Box 1234, Cobar 2835	<p>Treatment of personal information must be compliant with appropriate legislation and policy.</p> <p>Must be validated before including the AED in the dataset.</p> <p>Not recommended for use during latency-sensitive operations.</p>
AED_ALT_CONTACT_PERSON_NAME	<p>Description: Name of an alternate person to contact for AED data/maintenance.</p> <p>String: A full name of a person, which can include first names, middle names or initials, and last names. May be [2] to [255] characters.</p>	John Doe	<p>Treatment of personal information must be compliant with appropriate legislation and policy.</p> <p>Must be validated before including the AED in the dataset.</p>
ALT_CONTACT_PHONE_NUMBER	<p>Description: Phone number of AED_ALT_CONTACT_PERSON_NAME.</p> <p>Telephone number: ACMA-compliant format.</p>	+61 400 321 456	<p>Treatment of personal information must be compliant with appropriate legislation and policy.</p> <p>Must be validated before including the AED in the dataset.</p>
ALT_CONTACT_EMAIL_ADDRESS	<p>Description: Email address of AED_ALT_CONTACT_PERSON_NAME.</p> <p>Email address: The maximum length of the domain name is 255 characters, and the maximum length of the local part is 64 characters.</p>	JDoe from jjj.org.au	<p>Treatment of personal information must be compliant with appropriate legislation and policy.</p> <p>Must be validated before including the AED in the dataset.</p>

ALT_CONTACT_POSTAL_ADDRESS	Description: Postal address of AED_ALT_CONTACT_PERSON_NAME. May be different to AED location. String: Compliant with Australian Post standards.	PO Box 1234, Cobar 2835	Treatment of personal information must be compliant with appropriate legislation and policy. Must be validated before including the AED in the dataset. Not recommended for use during latency-sensitive operations.
AED_CONTACT_CREATED	Description: Date AED Contact fields were created. Date format: DD/MM/YYYY.	10/02/2022	Metadata: Supplied by system.
AED_CONTACT_UPDATED	Description: Each date AED Contact fields were updated. One entry per update. Date format: DD/MM/YYYY.	10/02/2022	Metadata: Supplied by system. May validly be blank if AED Contact fields have not been updated.

AED location details

The information provided in these fields may contain references to sensitive AED locations. The location details are intended to support uses including:

- location of accessible AEDs in an emergency (non-restricted locations)
- location of alternate accessible AEDs in an emergency (non-restricted locations)
- location verification and update (including input from crowdsourced input)
- AED maintenance
- planning of future AED locations.

Private owners of AEDs may validly have blank AED_HOLDING_ORGANISATION_NAME.

Restrictions on use: The fields containing sensitive location information should not be provided for public access. Access to sensitive location information should be provided only to trusted third parties who

have committed to treat location-sensitive information in a confidential manner, and only with the consent of AED_CONTACT_PERSON_NAME (or AED_ALT_CONTACT_PERSON_NAME).

Guidance on use: AED_UNIQUE_QR_CODE should only be generated and shared with AED_CONTACT_PERSON_NAME (or AED_ALT_CONTACT_PERSON_NAME) once all location information has been validated. If AED_CURRENT_LOCATION is '1' (not in reported location), then this invalidates the AED location information. It should be used as a trigger to update the AED location information. All applications of the dataset should report this location mismatch.

Quality requirements: Fields should not be blank unless explicitly included as a valid option. Fields should match Field Type. The AED_STREET_ADDRESS should be validated before inclusion of the AED in the dataset.

AED Location	Field Description and Type	Example	Sensitivity
AED_UNIQUE_IDENTIFIER	Description: Unique identifier of the AED in the dataset. Integer: Up to [10] digits.	12344321	Metadata: Supplied by system.
AED_UNIQUE_QR_CODE	Description: Unique QR code associated with AED in the dataset. QR code: ISO/IEC 18004:2015 compliant.		Metadata: Supplied by system. Should not be generated until all AED Location fields are valid. May validly be blank.
AED_STREET_ADDRESS	Description: Street address of the AED. String: Validated street address format.	26 Barrier Highway, Cobar, NSW, 2835	Must be validated (e.g. by NSW Spatial Services) before including the AED in the dataset.
AED_HOLDING_ORGANISATION_NAME	Description: Name of the organisation where the AED is located. String: A free text name of a business or organisation. May be 0 to [255] characters.	Cobar Cricket Club	May validly be blank.
LOCAL_LANDMARKS	Description: Landmarks that could help identify AED_STREET_ADDRESS. String: Free text. May be 0 to [255] characters.	Opposite Bowls Club	May validly be blank. Entries must be validated (e.g. by data custodian) before including the AED in the dataset.
AED_LOCATION_DESCRIPTION	Description: Free text description of where the AED is located within AED_STREET_ADDRESS. May include floor number. String: Free text. May be [10] to [1,024] characters.	In cabinet on wall, under AED sign in reception area.	May be sensitive information depending on AED_LOCATION_SENSITIVITY. Must be validated before including the AED in the dataset (e.g. by data custodian).
AED_LOCATION_SENSITIVITY	Description: Indication of the sensitivity of the AED location within AED_STREET_ADDRESS (e.g. restricted access area). Boolean: 0 – not sensitive 1 – sensitive		Access to information about AEDs in sensitive locations must be controlled.

AED_LOCATION_IMAGE	<p>Description: Photograph of AED location within AED_STREET_ADDRESS.</p> <p>Image: JPEG, GIF, PNG or BMP format. Maximum size [5MB].</p>		
AED_CURRENT_LOCATION	<p>Description: Indication if the AED is known to be in a different location to that described by AED_LOCATION_DESCRIPTION</p> <p>Boolean:</p> <p>0 – AED is in location</p> <p>1 – AED is not in location</p>	1	<p>This field will invalidate AED location information. It should be used as a trigger to update the AED location information.</p> <p>This field is not intended to track mobile AEDs.</p> <p>The AED should be removed from the dataset until this field is '0'.</p>
AED_COORDINATES	<p>Description: Numerical coordinates of AED location within AED_STREET_ADDRESS.</p> <p>Numeric: Latitude, longitude.</p>	-31.49° S, 145.83° E	<p>Must be validated (e.g. by data custodian) to AED_STREET_ADDRESS level before including the AED in the dataset.</p>
AED_LOCATION_CREATED	<p>Description: Date AED Location fields were created.</p> <p>Date format: DD/MM/YYYY.</p>	10/02/2022	<p>Metadata: Supplied by system.</p>
AED_LOCATION_UPDATED	<p>Description: Each date on which AED Location fields were updated. One entry per update.</p> <p>Date Format: DD/MM/YYYY.</p>	10/02/2022	<p>Metadata: Supplied by system.</p> <p>May validly be blank if AED Location fields have not been updated.</p>

AED accessibility details

The information provided in these fields may contain references to AED in sensitive locations. The accessibility details are used in conjunction with location details to support uses including:

- location of accessible AEDs in an emergency (non-restricted locations)
- location of alternate accessible AEDs in an emergency (non-restricted locations)
- accessibility verification and update (including input from crowdsourced input)
- planning of future AED locations.

Restrictions on use: The fields containing sensitive accessibility information should not be provided

for public access. Access to sensitive accessibility information should be provided only to trusted third parties who have committed to treat sensitive accessibility information in a confidential manner, and with the consent of AED_CONTACT_PERSON_NAME (or AED_ALT_CONTACT_PERSON_NAME).

Guidance on use: AED_ACCESS_HOURS_XX must be used in conjunction with AED_ACCESSABILITY; that is, if AED_ACCESSABILITY is not '0' (publicly accessible), then there are no public access hours.

Quality requirements: Fields should not be blank unless explicitly included as a valid option. Fields should match Field Type.

AED Accessibility	Field Description and Type	Example	Sensitivity
AED_ACCESSABILITY	<p>Description: Numeric indicator of the degree of accessibility of AED location within AED_STREET_ADDRESS.</p> <p>Integer:</p> <p>0 – publicly accessible</p> <p>1 – restricted to occupants of AED_STREET_ADDRESS</p> <p>2 – restricted by AED_LOCATION_SENSITIVITY</p> <p>3 – other restrictions</p>	2	Access to information about AEDs in restricted access locations must be controlled.
AED_ACCESS_RESTRICTIONS	<p>Description: Free text description of any restrictions on access to AED if AED_ACCESSABILITY is not '0'.</p> <p>String: Free text. May be 0 to [1,024] characters.</p>	Only accessible by XYZ staff due to access controls.	Validly blank only if AED_ACCESSABILITY is '0'.

<p>AED_ACCESS_HOURS_MONDAY</p> <p>AED_ACCESS_HOURS_TUESDAY</p> <p>AED_ACCESS_HOURS_WEDNESDAY</p> <p>AED_ACCESS_HOURS_THURSDAY</p> <p>AED_ACCESS_HOURS_FRIDAY</p> <p>AED_ACCESS_HOURS_SATURDAY</p> <p>AED_ACCESS_HOURS_SUNDAY</p> <p>AED_ACCESS_HOURS_PUBLIC_HOLIDAY</p>	<p>Description: Hours AED can be accessed by the public on days of the week and public holidays. Total of 8 fields.</p> <p>Time: Uses 24-hour format in local time zone of AED_STREET_ADDRESS.</p>	00:00-24:00	<p>Must be used in conjunction with AED_ACCESSIBILITY; that is, if AED_ACCESSIBILITY is not '0', then there are no public access hours.</p>
AED_CODE_REQUIRED	<p>Description: Any code required to access the AED, for example, a cabinet code.</p> <p>Boolean:</p> <p>0 - no code required</p> <p>1 - code required</p>	1	
AED_CABINET_ACCESS_CODE	<p>Description: Access code of the AED cabinet.</p> <p>Integer: May be 1 to [10] digits.</p>	0400	<p>Validly blank only if there is no code to access an AED or AED cabinet.</p> <p>Must be validated (e.g. by data custodian) before the AED is included in the dataset.</p>
AED_ACCESS_CREATED	<p>Description: Date the AED Access fields were created.</p> <p>Date format: DD/MM/YYYY.</p>	10/02/2022	<p>Metadata: Supplied by system.</p>
AED_ACCESS_UPDATED	<p>Description: Each date AED Access fields were updated. One entry per update.</p> <p>Date format: DD/MM/YYYY.</p>	10/02/2022	<p>Metadata: Supplied by system.</p> <p>May validly be blank if AED Access fields have not been updated.</p>

AED operational details

The information provided in these fields may contain references to AED in sensitive locations. The operational details are used in conjunction with location and accessibility details to support uses including:

- location of an operational AED in an emergency (non-restricted locations)
- location of alternate operational AEDs in an emergency (non-restricted locations)
- operational status verification and update (including input from crowdsourced input)
- AED maintenance alerts.

Restrictions on use: The fields containing sensitive accessibility information should not be provided for public access. Access to sensitive accessibility information should be provided only to trusted third parties who have committed to treat sensitive

accessibility information in a confidential manner, and only with the consent of AED_CONTACT_PERSON_NAME (or AED_ALT_CONTACT_PERSON_NAME).

Guidance on use: If any of AED_EXPIRY_DATE_XX entries are beyond the current date, all applications of the dataset should mark AEDs as past expiry data. These fields should be used to trigger a maintenance alert.

If either of AED_AMBIENT_XX are '1' (have been exposed to temperate or humidity outside of operational range), all applications of the dataset should mark AEDs accordingly. These fields should be used to trigger a maintenance alert.

Quality requirements: Fields should not be blank unless explicitly included as a valid option. Fields should match Field Type. AED_MODEL values should be selected from a closed (drop-down) list rather than free text.

AED Operational Information	Field Description and Type	Example	Sensitivity
AED_MODEL	Description: Brand and model. String: Manufacturer name and model of the AED.	Heartstart FR2	Preferably driven by selection from a closed list.
AED_SERIAL_NUMBER	Description: Serial number of the AED. String: manufacturer-specific serial number of the AED.	908284613-S	Validly blank only if AED_ACCESSABILITY is '0'.
AED_EXPIRY_DATE_WARRANTY	Description: Expiry date of the AED warranty. Date format: DD/MM/YYYY or MM/YYYY.	02/2023	If the MM/YYYY date format is supplied, the date format will be extended to 01/MM/YYYY.
AED_EXPIRY_DATE_BATTERY	Description: Expiry date of the battery as indicated by the AED. Date format: DD/MM/YYYY or MM/YYYY.	02/2023	If MM/YYYY date format is supplied, the date format will be extended to 01/MM/YYYY.
AED_EXPIRY_DATE_ADULT_PAD	Description: Expiry date of adult chest pads as indicated by AED. Date format: DD/MM/YYYY or MM/YYYY.	02/2023	If MM/YYYY date format is supplied, the date format will be extended to 01/MM/YYYY.

AED_EXPIRY_DATE_PAEDIATRIC_PADS	<p>Description: Expiry date of the paediatric chest pads as indicated by the AED.</p> <p>Date format: DD/MM/YYYY or MM/YYYY.</p>	02/2023	If MM/YYYY date format is supplied, the date format will be extended to 01/MM/YYYY.
AED_EXPIRY_DATE_SPARE_PADS	<p>Description: Expiry date of any (adult, paediatric) spare chest pads as indicated by the AED.</p> <p>Date format: DD/MM/YYYY or MM/YYYY.</p>	02/2023	If MM/YYYY date format is supplied, the date format will be extended to 01/MM/YYYY.
AED_AMBIENT_TEMPERATURE	<p>Description: Has the AED been exposed to temperatures outside of the operating temperature range since last reported on?</p> <p>Boolean: 0 – it has not 1 – it has</p>	1	This parameter is likely to be under-reported or inaccurately reported. Care should be taken with use of this parameter.
AED_AMBIENT_HUMIDITY	<p>Description: Has the AED been exposed to humidity outside of the operating humidity range since last reported on?</p> <p>Boolean: 0 – it has not 1 – it has</p>	1	This parameter is likely to be under-reported or inaccurately reported. Care should be taken with use of this parameter.
AED_OPERATIONAL_STATUS	<p>Description: Is the AED in operational condition?</p> <p>Boolean: 0 – it is not 1 – it is</p>	1	<p>This parameter relies on combinations of AED_EXPIRY_DATE fields and AED_AMBIENT fields.</p> <p>An AED reported as being operational must be consistent with the AED_EXPIRY_XX and AED_AMBIENT_XX fields.</p>

AED_NETWORKED	Description: Is the AED/AED cabinet connected to a communications network? Boolean: 0 – it is not 1 – it is	1	
AED_OPERATIONAL_CREATED	Description: Date AED Operational fields were created. Date format: DD/MM/YYYY.	10/02/2022	Metadata: Supplied by system.
AED_OPERATIONAL_UPDATED	Description: Each date AED Operational fields were updated. One entry per update. Date format: DD/MM/YYYY.	10/02/2022	Metadata: Supplied by system. May validly be blank if the AED Operational fields have not been updated.

AED crowdsourced input

These parameters are not mandatory for any AED in the dataset. These fields allow crowdsourced feedback on the location, availability, or operational condition of individual AEDs. One challenge is to consistently link the crowdsourced report to an AED registered in the dataset.

Crowdsourced input is not necessarily validated, so should be used as a flag to update, or validate AED status rather than replace. The ability to provide crowdsourced feedback should be open to everyone. Given the potentially sensitive nature of the information provided, crowdsourced should be treated as containing sensitive or personal information by default and so follow appropriate NSW legislation or policies. Once crowdsourced feedback is acted on, the relevant fields of the AED should be updated.

The information provided in these fields may contain references to AED in sensitive locations.

The crowdsourced details are used in conjunction with location and accessibility details to support uses including:


- operational status verification and update
- AED maintenance alerts.

Restrictions on use: The fields containing sensitive accessibility information should not be provided

for public access. Access to sensitive accessibility information should be provided only to trusted third parties who have committed to treat sensitive accessibility information in a confidential manner, and only with the consent of AED_CONTACT_PERSON_NAME (or AED_ALT_CONTACT_PERSON_NAME).

Guidance on use: All crowdsourced feedback should be treated as unconfirmed until validated by AED_CONTACT_PERSON_NAME (or AED_ALT_CONTACT_PERSON_NAME). Applications that use crowdsourced data should treat feedback as unconfirmed until validated. Linking crowdsourced data to a given AED_UNIQUE_IDENTIFIER may be done by matching AED_UNIQUE_QR_CODE, matching AED_COORDINATES or through data custodian validation. The scope of the crowdsourced feedback (location, access, operational condition) should be validated by the data custodian in conjunction with the AED_CONTACT_PERSON_NAME (or AED_ALT_CONTACT_PERSON_NAME).

Quality requirements: Fields should not be blank unless explicitly included as a valid option. Fields should match Field Type.

AED Crowdsourced Information	Field Description and Type	Example	Sensitivity
AED_CROWDSOURCED_STATUS	Description: free text description from a member of the public if they believe a registered AED location/ accessibility/operation condition is different from what it should be. String: Free text. May be [0] to [1,024] characters.		May validly be blank. Multiple AED_CROWDSOURCED_STATUS entries may be recorded per AED.
AED_CROWDSOURCED_IMAGE	Description: Photograph relevant to AED location. Image: JPEG, GIF, PNG or BMP format. Maximum size [5MB].		May validly be blank. Multiple AED_CROWDSOURCED_IMAGE entries may be recorded per AED.
AED_CROWDSOURCED_COORDINATES	Description: Numerical coordinates of AED location described in AED_CROWDSOURCED_STATUS. Numeric: Latitude, longitude	-31.49° S, 145.83° E	
LINK_TO_REGISTERED_AED	Description: Match (mostly likely) to registered AED_UNIQUE_IDENTIFIER if known. Integer: Blank or same format as AED_UNIQUE_IDENTIFIER.	12344321	Metadata: Supplied by system or data custodian. May validly be blank.
CONFIDENCE_LINK_TO_REGISTERED_AED	Description: Level of confidence in match to registered AED_UNIQUE_IDENTIFIER if known. Integer: 0 – unknown 1 – low confidence 2 – high confidence 3 – exact match	3	Metadata: Supplied by system or data custodian. Set to '0' if LINK_TO_REGISTERED_AED is blank.
AED_CROWDSOURCE_CREATED	Description: Date AED Crowdsourced fields were created. Date format: DD/MM/YYYY.	10/02/2022	Metadata: Supplied by system.
AED_CROWDSOURCE_UPDATED	Description: Each date AED Crowdsourced fields were updated. One entry per update. Date format: DD/MM/YYYY.	10/02/2022	Metadata: Supplied by system. May validly be blank if AED Crowdsourced fields have not been updated.

Creating the data asset

This section explores practical considerations of creating the dataset and managing data products across the data life cycle.

Figure 8 (page 17) shows a simplified data life cycle that allows us to explore controls that may be considered from the point of data creation to collection, storage and then use by the receiving entity. This 'use' may be any of the use cases provided earlier, including analysis of the data. The data or data products are then shared and finally archived. The simple life cycle can be expanded at any phase to more explicitly show the range of activities that take place during that phase.

This section focuses on the most relevant stages of the data life cycle.

Create/collect phase

Authority to receive and use data

Data is sourced from an individual responsible for an AED or uploaded from an existing dataset. Authority to receive, store and use data must be gained from one of AED_CONTACT_PERSON_NAME (or ED_ALT_CONTACT_PERSON_NAME) or the custodian of the existing AED Dataset.

In the case of an individual, consent to receive and use AED data can be confirmed through credentialled logon to Service NSW. In the case of an existing data ingest, consent to receive and use should be explicitly agreed and archived.

Data quality

Data sourced from an individual responsible for an AED should be entered via structured template forms that ensure data quality. This requires the NSW data custodian to validate some fields with AED_CONTACT_PERSON_NAME (or ED_ALT_CONTACT_PERSON_NAME).

Data sourced from an existing dataset will require the NSW data custodian to validate all data quality aspects. Data on individual AEDs should not be linked to the dataset until all data quality fields are validated.

Organise/store phase

When all data fields are validated for an individual AED, it can be registered in the AED Dataset. This may have implications for the AED Dataset metadata and for the data products created.

AED metadata

There are mandatory metadata fields for NSW datasets that contain spatial data. Metadata should be evaluated for the need to refresh as new AEDs are registered.

These include:

- Title – the name of the data layer. This will not change after creation of the dataset.
- Abstract – similar to the executive summary. This is not likely to change after creation of the dataset.
- Metadata contact organisation – organisation contact details for the metadata content. This will change over time as a result of reorganisation within government and role changes.
- Geographic location – the spatial extent of the data. This will likely change as new AEDs are registered in the dataset.
- Lineage – from which other data was this dataset created. This will likely change as new AEDs are registered in the dataset.
- Temporal extent – over what period was the data captured? This will change as new AEDs are registered in the dataset.
- Distribution format – data file format. This is unlikely to change.
- Keywords – words used for search and discovery of dataset. This is unlikely to change.
- Maintenance frequency – this is likely to change over time.
- Use limitation – guidance for use needs to reflect personal information and sensitive information in the dataset. This may change slowly over time.
- Legal restrictions – this may change slowly over time.

Data products

The base dataset contains personal information and (potentially) sensitive location information.

Three (virtual) data products which could be created include:

- raw data with personal information and sensitive location information (requires a high control environment)
- raw data without personal information and with sensitive location information (requires a high control or moderate control environment)
- raw data without personal information and without sensitive location information (suitable for a no control environment).

Access to these different data products should reflect the need to protect personal and sensitive information.

QR code creation

The creation of a QR code should not happen until an AED is registered to the AED Dataset. Once registered, the QR code should be emailed to AED_CONTACT_PERSON_NAME (or ED_ALT_CONTACT_PERSON_NAME). The QR code should be printed out and placed near the relevant AED.

At a minimum, the QR code should contain:

- AED_UNIQUE_IDENTIFIER.

Any additional fields should be tested for personal information or sensitive location information.

Analyse/use phase

This section highlights considerations for use of the AED Dataset. Uses include example use cases as described early in the appendix as well as 'using' the dataset for crowdsourced feedback and maintenance.

Crowdsourced feedback

Crowdsourced feedback can be offered by submitting a comment through Service NSW either as an identified individual or an anonymous individual.

The ability to provide crowdsourced feedback should

be open to everyone. The crowdsourced feedback linkage to an AED_UNIQUE_IDENTIFIER requires validation by the NSW data custodian.

Crowdsourced input is not necessarily validated, so should be used as a flag to update, or validate AED status rather than replace. Given the potentially sensitive nature of the information provided, crowdsourced should be treated as containing sensitive or personal information by default and so follow appropriate NSW legislation or policies. Once crowdsourced feedback is acted on, the relevant fields of the AED should be updated.

AED data asset maintenance

One use case of the AED Dataset is to analyse for those AEDs which have AED_EXPIRY_DATE_XX fields out of date, AED_AMBIENT_XX out of range or AED_OPERATIONAL_STATUS as non-operational. Identification of such AEDs should trigger a prompt to the AED_CONTACT_PERSON_NAME (or ED_ALT_CONTACT_PERSON_NAME).

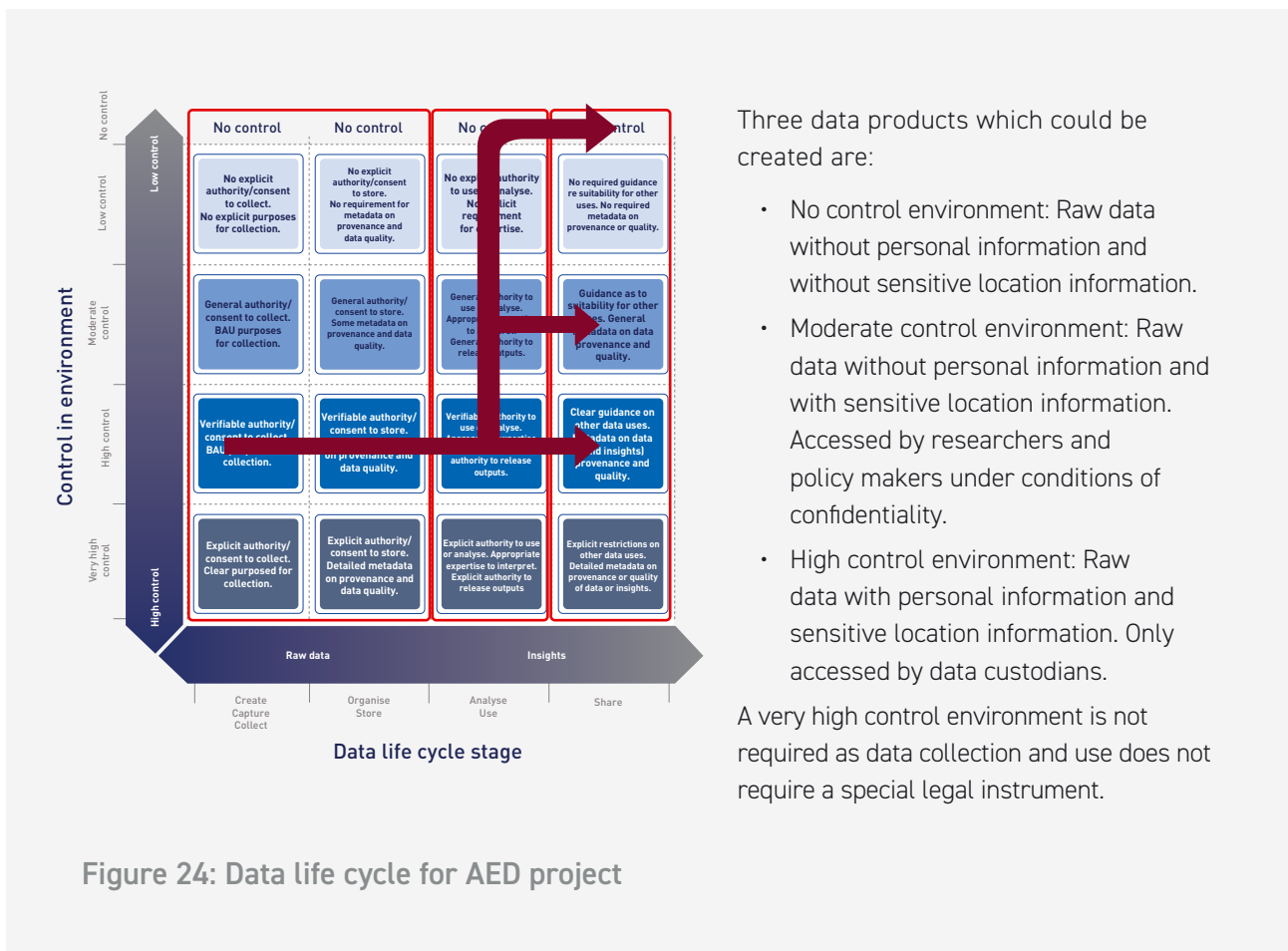


Figure 24: Data life cycle for AED project





About the Australian Computer Society

ACS is the professional association for Australia's technology sector.

We represent technology professionals across industry, government and education. Our aim is to grow the nation's digital skills and capacity.

Wherever you may be in your tech career, ACS has the solution to suit your needs and take your career forward.

Plan your career

Assess and profile your current skills, understand your competencies, get recognised as a Certified Professional and map your career plan.

Learn new skills online

Gain new skills across cyber security, cloud tech, AI, machine learning and more, with over 8,000 flexible online videos and courses.

Grow your tech network

Meet the right people – network with other tech professionals as well as leaders from some of the biggest local and global organisations.

Stay up to date and relevant

Stay informed on industry trends and emerging technologies with over 200 events, masterclasses, research projects and case studies.

Be inspired by industry leaders

Join mentoring programs designed to accelerate your career growth. ACS mentors are leaders who are here to help guide you.

Protect yourself

Stay protected with comprehensive liability insurance.

Have a voice

On behalf of tech professionals ACS engages with media and policy makers on the issues affecting the technology sector, along with providing a range of resources to educators and industry to boost the nation's digital capabilities and competitiveness.

Unlock your potential – find out more about joining ACS at acs.org.au.

Contact us

General enquiries

E: info@acs.org.au

T: +61 2 9299 3666

