CADRE Five Safes Framework

Conceptualisation and Operationalisation of the Five Safes Framework

DOI: 10.5281/zenodo.5748611

Dr Steven McEachern (Editor), Version 1.0, November 2021
Australian Data Archive, Centre for Social Research & Methods
The Australian National University

Figures List

Tables List

Executive Summary

The CADRE Five Safes framework is an output of the CADRE (Coordinated Access for Researchers, Data and Environments) Platform project. The CADRE framework includes the conceptual underpinnings and the guardrails for sensitive data access management and the range of information associated with the Five Safes principles that can be operationalised in a decision-support system.

- In the *Introduction* and *Context* sections the CADRE Platform project and the social science research data management practices associated with sensitive quantitative and qualitative data are outlined.
- In the *Conceptualisation* section a full exploration is undertaken of: the uptake of Five Safes framework in Australia; the concepts from the Five Safes framework i.e., projects, people, data, settings and outputs; additional concepts i.e., organisations and groups; and key intersections and alignments of these concepts.
- In the *Operationalisation* section the information requirements associated with managing sensitive data access requests and provisioning research environment services for sensitive data analysis are evaluated and initial information and data models are proposed for the CADRE information exchange.
- In the *Appendices* the user requirements from project partners helping to develop the CADRE Platform are summarised and sensitive data categorisations are collated.

Introduction

CADRE Project

The CADRE project aims to develop the integrated infrastructure required to implement the Five Safes framework in Australian research institutions and collaborating government and private sector agencies. This new framework is being adapted for use by the Office of the National Data Commissioner, and new legislation and data governance frameworks are being designed and developed to reduce barriers to access to data held by government while maintaining public trust that sensitive data is only being released and used appropriately. A central and critical element of this will be the Five Safes framework, which will provide a basis for the release of government data. The new CADRE platform will enable data owners and users to address the core concerns around governance, creation, management and sharing of sensitive data for research. As a result, Australia's research sector will have improved access to the data needed to develop solutions to a wide range of public problems.

Purpose of this Paper

The purpose of this paper is to provide a conceptual framework to underpin the CADRE Five Safes infrastructure platform. The CADRE platform is being developed to improve Australian researcher access to sensitive data, to fill a gap in national research infrastructure, remove barriers and enhance data access processes. This will be achieved by operationalising the Five Safes framework being adopted in the Commonwealth government, based on international best practices. The underlying premise of the Five Safes is a data access management framework. The "Safes" themselves are posited as a series of dimensions, outlined in Table 1 (Desai et al., 2016):

Safe projects	Is this use of the data appropriate?
Safe people	Can the researchers be trusted to use it in an appropriate manner?
Safe data	Is there a disclosure risk in the data itself?
Safe settings	Does the access facility limit unauthorised use?
Safe outputs	Are the statistical results non-disclosive?

While the framework has provided an effective basis for principles-based approaches to supporting data access, particularly in the government sector, there is wide variation in the understanding and interpretation of each dimension.

This paper is therefore intended to cover three overarching topics:

- A **background** to the Five Safes and its use in Australia and internationally
- A **conceptual framework** for the Five Safes within the context of the CADRE project
- The **application of the framework** to a series of use cases from CADRE partners

The paper is structured in three parts:

> *Five Safes – Contextualisation* – a review of the history of the Five Safes framework and its uptake internationally and in Australia to assist with the development of data access services and research support.

> *Five Safes – Conceptualisation* – an examination of each safe concept in terms of the function that concept plays in within the Five Safes and how the combination and recombination of concepts serve as underpinnings for ethical considerations.

> *Five Safes – Operationalisation* – a description of existing processes and the information sought and collated to manage sensitive data access requests and manage the provision of a project workspace to use sensitive data in research environments.

Two user viewpoints are brought together around research support:

> That of a **data custodian/broker** when managing sensitive data access requests by researchers.

> That of an **infrastructure service provider** when managing the environments where researchers are using sensitive data in research.

Acknowledgements

This paper is the result of the combined efforts of the Conceptual Working Group of the CADRE Project. The working group met on a fortnightly basis from May to October 2021 to review the existing Five Safes literature and concepts and to discuss applications and extensions of the framework to their specific use cases and the Australian context more generally. Participants in the working group included:

- Dr Steven McEachern, Dr Heather Leasor, Marina McGale & Ingrid Mason, Australian Data Archive, Australian National University
- Jatender Mohal, Australian Institute of Family Studies
- Prof Julie McLeod, Dr Kate O'Connor & Nicole Davis, SOCEY, University of Melbourne and La Trobe University
- Shiree Heath, ERICA, Centre for Big Data Research in Health, UNSW
- Greg D'Arcy, AARNet

Context

Background

Social science researchers in higher education generate, use and manage access to sensitive quantitative and qualitative data that contains information about people. Different curatorial practices and privacy concerns associated with data sharing have evolved due to the nature of the different data types and the digital research methods associated with quantitative and qualitative social science research practice.

An examination of the emergence of the Five Safes framework in the history of quantitative social science research and its critical relationship with national statistics agencies, and the history of qualitative social science research and its critical relationship with national cultural agencies, together forms a comparative analysis of the sensitive data access management practices of social science researchers in higher education in Australia.

The historical recounting and the explanation of the ethical bases on which to establish common ground and a shared system for sensitive data access management (whether quantitative or qualitative data) is founded on an assumption that the Five Safes framework has broader applicability. It is anticipated that external review from peers in Australian and international social science research networks will provide vital critical feedback on the validity of the findings of the CADRE Conceptual Working Group.

Quantitative Data

Enabling access to research and government data has a long history in the social sciences. Social science data archives were established as early as the 1920s to support access to data for research purposes, and numerous national social science archives were established by the 1960s across Europe and North America to facilitate data sharing for research purposes (Shankar et al., 2016; Green and Gutmann, 2007).

National statistical services have similarly long histories of supporting access to data for research. The Australian Bureau of Statistics (ABS) for example has published tabular aggregate data since its inception (ABS, 2011). With the advent and diffusion of mainframe computers and database systems in the 1960s, computation against data about individuals became increasingly viable as a means of social science research. Statistical offices developed unit record files – data files with individuals as rows and variables as columns – for use in scientific research. These data files were disseminated for use, often as machine tapes for use in the new mainframe systems. Progressively as new and varied dissemination systems became available, unit record files were shared through varying means, with the advent of the internet enabling much greater opportunity for dissemination through both hypertext and file transfer protocols.

Desai, Ritchie and Welpton (2016) note that data access within government has generally been managed through two approaches – (1) the signing of access agreements controlling use of the data through contractual arrangements (such as Deeds and Memoranda of Understanding), or through (2) management of “scientific use” deidentified data files (also known as “confidentialised unit record files”) for use in research. Often access involved a combination of the two approaches – for example within the Australian Commonwealth Department of Social Services a combination approach was used to enable researcher access to the longitudinal studies supported by the National Centre for Longitudinal Data (Ritchie and Green, 2016). Alongside these approaches, in circumstances where data could not be reasonably disseminated outside the custodian organisation, secure physical facilities were also established to allow data users to come on site to conduct analysis in a controlled environment (Desai et al., 2016; Trewin et al., 2007).

For much of the 20th and early 21st century, these broad approaches largely satisfied the needs of both data providers and users. The advent of the internet did however bring additional capability which meant that these approaches were no longer seen as sufficient. The increasing availability and sophistication of computation and analysis systems however added new complexity to the frameworks for managing data access. The growth in both data sources which provide potentially identifying information, along with computational resources and algorithmic methods for the use of these additional sources, has been demonstrated to render some of the previous methods less suitable in the current social and technical context (Culnane et al., 2017). Additionally, new secure access methods such as remote access facilities and remote processing environments (Sax Institute, n.d.; NORC, n.d.) has meant that new options were emerging that allowed providers and users to consider a broader range of access options and opening up new possibilities for data access and user support.

The purpose of the Five Safes

It was within this context that the Five Safes framework was established. The Five Safes is a principles-based framework for the management of access to sensitive data. Originally established in 2003 as a model for the provision of access to unit record data from the Office of National Statistics in the United Kingdom, it is increasingly recognised in both research and government circles as a best-practice model for public sector data custodians (Office of the National Data Commissioner, 2019), and across the research sector (O'Hara, 2019).

The Five Safes framework was intended to be able to address these limitations by providing a principles-based framework for managing decision-making regarding data access. The framework was originally established by Felix Ritchie in 2003, during his time as director of the Virtual Data Lab of the Office of National Statistics (ONS) in the United Kingdom, and progressively adopted by the UK Data Archive as the Data Lab program expanded from the Official Statistics community to the academic community in the UK.

International Best Practice

From these foundations, the Five Safes framework has progressively been adopted across both the official statistics and social science data archives communities, and from there progressively in government and research data communities more broadly. Within the official statistics and government data communities, the Five Safes now forms the foundation of at least three national statistical offices' access frameworks – the United Kingdom (ONS, 2017), Australia (ABS, 2017) and New Zealand (Statistics New Zealand, 2020) – as well as major statistical agencies in Germany (Müller and vom Berge, 2020) and

Australia (Australian Institute of Health and Welfare, 2021) and the International Monetary Fund (Dabla-Norris et al., 2020). A more detailed discussion of the adoption in Australia is presented in the Five Safes – Conceptualisation section.

Qualitative Data

Qualitative data, particularly in the humanities, arts and social sciences (HASS), has often been more difficult to access than quantitative data due to a number of factors. Qualitative data covers a wide range of research data across HASS and into the sciences, including medicine, psychology etc., such as "case studies, personal experience, life stories, interviews, observations, and cultural texts" (NHMRC 2018b, p.103). A vast amount of pure qualitative research data is held by individual researchers or groups in universities; research centres, including government organisations such as the Australian Institute of Family Studies (AIFS) and the Australian Institute of Health and Welfare (AIHW); and traditional archives and other government, university and non-government cultural sector GLAMR (galleries, libraries, archives, museums, records) institutions. As explored in McLeod et al. (2020, p.4–5) there are a range of barriers to the archiving, sharing and reuse of qualitative data, particularly in the HASS academic community, ranging from technological to epistemological obstacles.

This wide range of locations in which qualitative research data might be found can itself be a barrier to other researchers attempting to locate data. In the GLAMR sector, including traditional archives services e.g., National Archives of Australia, there is a significant push to digitise and make open historic documents (much of which constitute qualitative data). These digitised items are held on individual collections online sites and accessible via aggregators such as Trove provided by the National Library of Australia or Victorian Collections provided by Creative Victoria. This push has made these data in cultural collections much more accessible to researchers, although there are still vast arrays of material not digitised due to staffing and funding issues. There are still constraints such as the researchers need to understand the structure and searching mechanisms of these repositories but this is made more accessible through training, staff assistance and information guides provided by the organisations.

By comparison, the academic HASS community has generally been slower to embrace idea of sharing and re-use of qualitative research data in an online environment. One of the main barriers to researchers making these available are concerns about who might access and use these data, how easily they might be accessed, and how privacy of their participants and third parties involved can be maintained (McLeod et al. 2020, p.5). This has led to a lower uptake in the digitisation and sharing of data by HASS researchers. This is gradually changing with funding bodies and universities requiring the digital archiving of data and the recommendations to consider making that data available for sharing and re-use. Researchers too increasingly see the benefits of making their data more accessible to others.

While most academic and government researchers must follow data management plans, there are varying requirements for digital storage of their research materials. Data governance does not necessarily require them to store this in a specific data repository. In universities, much research data is stored within a school/department computer share drive or in the university-run or approved repository. Some researchers or research teams choose to store in other wider repositories, most prominently in Australia, the Australian Data Archive (ADA), or they might be accepted for storage in the university archives. Other bodies that do qualitative or mixed-mode research, such as the AIFS, also store data in their individual repositories or with repositories such as the ADA.

Additionally, often historical qualitative data is stored in analogue form and held by the researcher. As with the GLAMR sector's push to digitise historic qualitative data in their collections, without such a movement within HASS fields, such data might not only be rendered less accessible but also lost over time.

Thus, a large percentage of qualitative research data is not readily findable or accessible to outsiders, including other researchers. The CADRE platform is an opportunity to widen access to the rich data held by various researchers and bodies. But, without uptake from diverse organisations, including government, universities, data repositories, other research groups and perhaps even cultural organisations, as well as deposit of qualitative data into larger research repositories such as the ADA, much of these data will continue to be difficult to access.

The CADRE Project

The foundations of the CADRE project lie in the adoption of the Five Safes in the government and academic sectors here in Australia. Within the Commonwealth jurisdiction, the Office of the National Data Commissioner (ONDC) has been established to streamline how public sector data is used and shared, both within government, and with researchers outside of government. To achieve this, ONDC are developing new legislative and data governance frameworks which are designed to reduce barriers to access to data held by government and improve data access, while maintaining the trust of the public with regards to their data. A central and critical element of this will be the Five Safes Framework, which will provide a basis for the release of government data and likely other sources (including research and commercial data).

While the ONDC work program will provide a new foundation for access to government data in Australia, a technical and social infrastructure for implementing the new framework does not currently exist. There will be substantial challenges to scaling the access procedures required, establishing, and linking the technologies required for secure access, and connecting the access procedures to the secure access technologies required to store and analyse the data. Unless these issues are addressed the expected value that can be gained from improved access will not be realised, and trust is likely to be further eroded.

This then is the purpose of the CADRE platform. CADRE will provide an operational model that responds to and overcomes these sensitive data access management challenges across sectors. The CADRE project will establish a shared and distributed access request management platform for the social sciences and related disciplines, to enable data owners and users to address the core concerns around governance, creation, management and sharing of sensitive data for research. The platform will standardise sensitive data request management documentation, provide decision-support and enable interoperability.

The core of the CADRE platform is built through the adoption of well-established protocols and technologies in Australian and international research infrastructure. The CADRE platform brings together existing identification services (e.g., DOI, ORCID, ROR and RAID) and accreditation frameworks arising from new federal legislation (i.e., the Data Availability and Transparency Bill); and integrates them with prevailing authentication and authorisation technologies to establish the CADRE platform in a shared information exchange environment. Leveraging these existing identifier services, frameworks and technologies is what makes it possible for the CADRE platform to enable a transformative change in research using sensitive data.

The development of the CADRE platform occurs in three phases:

1. **Conceptualisation** – the development of the conceptual framework and the information exchange protocols.
2. **Development** – the development of the data access management platform (CADRE) and integration with partner platforms (pilots).
3. **Operations** – the partner platforms move into production with the CADRE platform and additional pilots (integrations) commence.

In phase one (protocols development and system requirements) a consultation and business analysis program is undertaken for the development of the shared information model and user requirements.

In phase two (protocol adoption and pilot services) the adoption of the CADRE protocols for information sharing commences. The CADRE information exchange service will be developed by the CADRE core team (ADA, Australian Access Federation (AAF) and the Research Graph Foundation (RGF)), and test implementations are authenticating against the pilot service will developed by key CADRE partners, including ADA (Dataverse), AURIN (AURIN Portal) AARNet (Sensitive Data Service), and SODA Lab (Data CO-OPS).

In phase three (service operations) based on the outcomes of the pilot service and manual implementation, service providers will establish full connectivity to the CADRE authentication system, and data users (researchers) will be able to manage their request and accreditation processes through authentication to the full service.

CADRE Framework Design

The establishment of the CADRE platform requires a foundation of core identifier services, information systems and technologies to be adopted and adapted, to meet the needs of a mix of stakeholders: researchers, data owners/brokers, and research infrastructure service providers, that share a common goal in expediting access to sensitive data and thereby enabling research. This conceptual framework is the first of the outputs of the project, providing a set of guiding principles and stakeholder inputs for the overall design of the administrative and technical systems underpinning the CADRE information exchange.

The CADRE framework design enables critical reflections on the Five Safes concepts in the context of:

- increasing access to data (with mounting privacy disclosure concerns),
- social and legislative response (with interests in tension around unlocking personal data), and
- rapidly evolving technologies (with innovations in remote and controlled access).

The framework design brings together theory and practice around management of sensitive data, authorisation (and the chain of custody) and draws upon data and research workflows that operate within research and data lifecycles across multiple systems (an ecosystem). The design guides the development of the information architecture and the protocols for decision-support in the CADRE information exchange.

There is no literal translation of the Five Safes in the CADRE information architecture, rather conceptual framing serves as a lens, and aids in the identification of key intersections and alignments (of "Safes" and safety information) to include in the architecture of the information exchange.

Five Safes – Conceptualisation

The Five Safes in Australia

As the Five Safes model has progressively been adopted internationally, it has taken some time for the uptake to occur in Australia. Here we consider the use of the Five Safes in the Australian context, and its current usage in terms of usage in Australian government and academic policy and practice.

Australian Foundations

There have been two key elements in Australia to the adoption of the Five Safes model. The first area of activity was the program of revisions to the Australian Bureau of Statistics confidentiality and data access frameworks. The first public expression of this activity came in 2017, with the publication of the "ABS Confidentiality Series" in August 2017 (ABS, 2017). This publication outlined the ABS' adoption of the Five Safes, along with some worked examples of each of the Five Safes as applied to variations of ABS published outputs. This publication highlighted the importance of confidentiality of individual participants in the statistical data production process. Here the ABS (2017) define confidentiality as:

> *protecting the secrecy and privacy of information collected from individuals and organisations*

The publication outlines a series of key indicators of potential disclosure risk, along with methods for the treatment of data to address confidentiality and privacy concerns. At the same time the publication also notes that the application of privacy-preserving methods brings with it a trade-off – namely the trade-off between confidentiality of the participant, and the utility of the data for public decision making and research data analysis. The paper also recognises a key characteristic of data disclosure – that the risk should be managed, rather than eliminated. The management of the privacy-utility trade-off (ABS, 2017) then is one of balancing these competing interests:

> *Managing disclosure risk becomes a question of assessing not only the data itself, but also the context in which the data are released. Once the context is clearly understood, it is much easier to determine how to protect against the threat of disclosure. The Five Safes Framework provides a structure for assessing and managing disclosure risk that is appropriate to the intended data use.*

This risk management approach then set the foundation for the application of the Five Safes framework within the ABS.

The second key driver of the use of the Five Safes was the Productivity Commission's enquiry into "Data Availability and Use". The Commission was instructed to undertake the enquiry in March 2016, with the final report of the Commission published in March 2017.

This report is notable for several reasons, as it set the foundations for several key initiatives in the Commonwealth government which have driven data management practices in the intervening five years since its publication. Of note were the following:

- The report outlines a possible institutional framework for the management and regulation of data sharing in the public sector. In particular, the report proposes a National Data Custodian, a set of "Accredited Release Authorities", and a framework for trusted and public users. These three institutions are all to be established (albeit with slightly different naming) as the key parties in the *Data Availability and Transparency Bill* (2020) currently before the Commonwealth parliament.

- The report clearly positions the Five Safes as the foundation of a data access framework for public (government) data. Chapter Four of the Commission's report introduces the Five Safes model, while Chapter Six ("Sharing and Releasing Data for Public Benefit") considers the application of each of the Five Safes to the provision of Australian public sector data. This model has now also been adapted (as "Data Sharing Principles") and included in the *Data Availability and Transparency Bill* – the enabling legislation for the establishment of both the data sharing framework and the ONDC. This bill is discussed further in the next section.

- The report also provides a possible application of the frameworks above to publicly funded data – explicitly referencing data generated by academic research that is funded through public grants (such as the Australian Research Council). While this proposal was not taken up by the Commonwealth in their implementation of data sharing policy, it has impacted on the policy development of specific research institutions (see examples in Australian Higher Education Research section).

One other element of the Productivity Commission report is of note. While outside of the direct purview of this paper, the report produced for the Parliament of Australia (PA) also establishes a framework for the consideration of consumer rights over data concerning themselves (PA, 2020, Chapter 5). The policy implications of this consumer framework have been taken up by the Australian Competition and Consumer Commission – which may have future implications for the management of data about individuals into the future, and hence impacts on the context of data sharing.

Australian Legislation

Having established the foundations of the Five Safes data sharing framework and potential institutional arrangements for the management of access to Commonwealth data through the Australian Bureau of Statistics and the Productivity Commission, the Commonwealth Department of Prime Minister and Cabinet has subsequently progressed with the development of policy and legislation to implement these proposals across the Commonwealth agencies.

More recently, the Office of the National Data Commissioner (ONDC) (2019) has adapted the Five Safes to the Australian data sharing context, defining each of their "Data Sharing Principles" as follows:

- **Projects**: Data is shared for an appropriate purpose that delivers a public benefit.
- **People**: The user has the appropriate authority to access the data.
- **Settings**: The environment in which the data is shared minimises the risk of unauthorised use or disclosure.
- **Data**: Appropriate and proportionate protections are applied to the data.
- **Output**: The output from the data sharing arrangement is appropriately safeguarded before any further sharing or release.

There is legislation currently before the Australian Parliament that will enshrine the "Data Sharing Principles" developed by the ONDC into legislation, the *Data Availability and Transparency Bill* (DAT Bill). Introduced to the Parliament in December 2020, the DAT Bill (formerly the *Data Sharing and Release Bill* 2020) proposes three key institutions with formal roles in data sharing – the "Data Scheme Entities" (PA, 2020):

1. The **National Data Commissioner**, with responsibilities for regulation of public data sharing, along with the provision of advice and guidance (PA, 2020, Section 39).
2. **Accredited Users**, who "are able to collect and use shared data (including by creating output they can share with third parties)" (PA, 2020, Section 11, Note 1).
3. **Accredited Data Service Providers**, "expert intermediaries who can assist data custodians to prepare and share data appropriately" (PA, 2020, Section 11, Note 1).

The DAT Bill will provide the framework for the management and regulation of datasets released under the framework. This includes reporting requirements on the Data Commissioner within their regulatory role. In Note 1, Section 33, the DAT Bill states:

> *The Commissioner must maintain a publicly available register containing the names of parties to each data sharing agreement and the mandatory terms included in the agreement*

The information transfers associated with the management, processing and reporting of data sharing agreements is notably one of the likely points of interaction between CADRE and the National Data Commissioner into the future.

Alongside the Commonwealth adoption of the Five Safes framework, there are also similar cases of adoption occurring at the state level in Australia. The earliest of these was in South Australia. There the Five Safes are embedded within the "Trusted access principles" specified in Part 4 of the *Public Sector (Data Sharing) Act 2016* (GSA, 2016). The framework has also been adopted in New South Wales (Data.NSW, 2020) and Victoria (GV, n.d.). While the Five Safes are not directly embedded in legislation in New South Wales, such as the Data

Sharing (Government Sector) Act 2015 No 60, the principles are directly specified in the public information from the NSW Data Analytics Centre and other New South Wales government agencies (Data.NSW, 2020).

Australian Higher Education Research

Compared to the Government sector, the academic sector has been much less formalised in the adoption of the Five Safes framework. There is explicit recognition of the Five Safes within several prominent examples across the sector, but the framework does not have a formal status of the Five Safes within key regulatory arrangements within the higher education research sector in Australia.

In terms of the legislative and regulatory frameworks for the management and oversight of academic research, there are two key regulatory statements – the *Australian Code for the Responsible Conduct of Research*, produced by the National Health and Medical Research Council (NHMRC, 2018a) and the *Statement on the Ethical Conduct of Human Research* (NHMRC, 2018b). There is also an additional set of ethical requirements associated with the conduct of research with First Nations (Aboriginal and Torres Strait Islander) peoples, outlined by the Australian Institute for Aboriginal and Torres Strait Islander Studies (AIATSIS) – the *Code of Ethics for Aboriginal and Torres Strait Islander Research* (AIATSIS, 2020).

None of the three regulatory statements above make direct mention of the Five Safes, although the Australian Code incorporates a reference to the Five Safes framework in the additional resources for their guide for researchers on "Management of Data and Information in Research" (NHMRC, 2019). This absence is however not altogether surprising. Notably the three regulatory statements are oriented primarily towards the conduct of academic research overall, rather than explicitly focussed on data sharing. The NHMRC Statement does address questions of data sharing and re-use in Chapter 3, under their "Element 4: Collection, Use and Management of Data and Information". The statement strongly recommends the use of a data management plan for the management of research data produced by or used in the project, and outline a series of key considerations (NHMRC, 2018b, s 3.1.46) that should be addressed in the plan, including but not limited to:

(a) "physical, network, system security and any other technological security measures;
(b) policies and procedures;
(c) contractual and licensing arrangements and confidentiality agreements;
(d) training for members of the project team and others, as appropriate;
(e) the form in which the data or information will be stored;
(f) the purposes for which the data or information will be used and/or disclosed;
(g) the conditions under which access to the data or information may be granted to others; and
(h) what information from the data management plan, if any, needs to be communicated to potential participants."

A number of these considerations in the data management plan align closely with the Five Safes framework. The NHMRC Statement also requires researchers to comply with any legal responsibilities associated with data that they create or use in their projects in section 3.1.47 (NHMRC, 2018b):

> *Researchers must comply with all relevant legal and regulatory requirements that pertain to the data or information collected, used or disclosed as well as the conditions of the consent provided by participants.*

The implication of this requirement is that it gives effect to obligations on researchers when they make use of data released under a Five Safes model - academic researchers will need to comply with any requirements emerging from the DAT Bill, and similarly for data from other jurisdictions.

The implications for the academic sector as custodians and creators of data are however less clear. This is not to say that the framework is not in use, or that it is not being incorporated into research practices. The adoption is however at a lower level, either at the level of the institution or research project. Examples here include:

- Griffith University research support training programs that include units on the Five Safes framework (Weaver and Richardson, 2021)
- The University of Queensland (UQ) links to the ABS Five Safes framework in their advice to researchers on Data, Materials and Records Management (UQ, 2020)
- Curtin University incorporation the Five Safes framework into the management of their secure research platform, SeRP@Curtin (Curtin University, n.d.)
- Projects such as the Health Information Workforce Census (Butler-Henderson et al., 2018) and Generation Victoria (Generation Victoria, 2019), incorporating the Five Safes framework directly into their data management and access protocols

There is also uptake of the Five Safes among research infrastructure providers within the Australian research sector. CADRE project partners including the Australian Data Archive (McEachern, 2018) and the Centre for Big Data Research in Health, developers of the ERICA platform (Churches and Jorm, 2019) make use of the Five Safes framework in the implementation of their data access protocols at each organisation.

Framework Structure

The foundations of the Five Safes are outlined in a series of papers by Ritchie and colleagues (Ritchie, 2017; Desai et al., 2016). The "Safes" themselves are posited as a series of dimensions, outlined in Table 1 (Desai et al., 2016):

Five Safes	Question	Joint Assessments
Safe projects	Is this use of the data appropriate?	Safe project – Safe data
Safe people	Can the researchers be trusted to use it in an appropriate manner?	Safe people – Safe project
Safe data	Is there a disclosure risk in the data itself?	Safe data – Safe project
Safe settings	Does the access facility limit unauthorised use?	Safe setting – Safe person
Safe outputs	Are the statistical results non-disclosive?	Safe output – Safe data

The premise underlying these five dimensions is that they can be considered both severally and jointly in the analysis of a data access system. As Ritchie (2017) suggests:

- Dimensions are designed so that each can be evaluated independently of the others, as far possible.

- All five dimensions need to be considered jointly to evaluate whether a data access system can provide an 'acceptable' solution.

A more detailed analysis of each "Safe" and conceptual intersections are explored in response to the collective (and various) needs of stakeholders for decision-support in the CADRE platform. The development of these "Safe" definitions is based on a review of the extant literature on the given "Safe" dimension, along with a series of guided discussions among the participants of the CADRE Content Working Group (CWG).

For the purposes of this work, the discussion focuses initially on the Five Safes as originally specified by Ritchie and colleagues (Desai et al., 2016). The interpretation of these within the Office of the National Data Commissioner's "Best Practice Guidelines" (ONDC, 2019) is considered relative to the original framing and Australian applications.

Finally, a set of potential indicators for each Safe dimension is identified as critical information for decision-support.

- Five Safes – the **original specification** to support research with sensitive data

- Five Safes – **translated as best practice guidelines** applied in the Australian context

- Five Safes – **Safety information and indicators** arising out of that application

Before looking at specifics of the Five Safes as a conceptual framework, it is useful to consider the basis on which indicators of each Safe were established by the CADRE Content Working Group. The initial discussion within the group focussed on the articulation of a possible definition of each Safe and its constituent requirements. It soon became apparent however that the level of safety expected was not common across the working group members – each of whom had responsibility for custodianship of data as part of their work responsibilities (within the chain of custody). The conclusion of the CADRE CWG was that there is unlikely to be a common approach that could be adopted by all users of the CADRE conceptual framework.

As an alternative, the question was raised as to whether specific elements of what be incorporated into an assessment of a Safe Project could be articulated. This change of approach allowed the CWG to thus establish a foundation for what key information might data custodians seek in order to make an assessment of the level of safety of the proposed use of the data (in a project or for student course work). This turns out to be a viable approach, and one that was adopted across all the Five Safe dimensions. Rather than seeking consensus on "What is Safe ____?", the group instead examined "What information will I need to make an assessment of safe ____?". This approach has enabled the CWG to establish the information requirements as a foundation for the information model to be developed for the CADRE information exchange.

Safe Project

An assessment of a Safe Project involves the question of the "suitable" use of the data. As Desai et al. (2016) note, this generally "… refers to the legal, moral and ethical considerations surrounding use of the data". In the context of public sector data use, this has often been translated in terms of public benefit (ONDC, 2019), and the translation of the Safe Project principle within the DAT Bill exposure draft consultation paper released by the Department of Prime Minister and Cabinet (PM&C) through ONDC (2020, p.14) directly requires an assessment of whether a proposed use is in the public interest:

> *data is shared for an appropriate project or program of work, including consideration of the public interest, and ethics, while maintaining strong privacy safeguards*

The question of what constitutes suitable use is highly subjective and is a notable challenge of the Safe Projects dimension. An example here is whether a project intended to derive commercial benefit from analysis of the data produced for non-commercial research purposes constitutes a suitable purpose. For the SOCEY use cases (based largely on qualitative data) in the CADRE group, such use was likely to be considered unacceptable – and therefore unsafe. By comparison, government agencies may be more open to the commercial exploitation of their data where overall public benefit might be derived – a position proposed in the Productivity Commission report and reflected in the government response to the Report (PM&C, 2018).

Notably, Ritchie and Tava (2020) also consider whether the Safe Project assessment is the one Safe that might be given priority above the other four in the Fives Safes framework.

There was agreement that the range of indicators which may be needed to describe the Safe Project would be diverse across the different CADRE user communities. The ONDC provide a possible approach to this problem in their *Best Practice Guide to Applying Data Sharing Principles* (2019), outlining a series of questions a data custodian might consider in their assessment of a project. The ONDC outline "Questions to ask" to ascertain the safety of a project and a similar approach can be considered for the CADRE implementers.

Table 1 Questions to Ask (Source: ONDC, 2019, Table 2)

Questions to ask: Project Principle
1. Is the project in the public interest and does it satisfy a purpose test?
2. Has all relevant information been provided to support assessment of the project proposal (e.g., who will access the data, for what purpose, over what period of time and what will happen to the data when the project ends)?
3. What processes or governance arrangements are needed to assess, monitor and oversee the project?
4. Who will make the assessment of whether to proceed with the project and do they possess the right capabilities to make the assessment?
5. Are there any restrictions (e.g., legal or data custodian imposed restrictions) on how the shared data may be used?
6. How will communication with applicants before and during the assessment of the project proposal be managed to maximise the likelihood of approval? What feedback will be provided?
7. Does there need to be ethics approval from a governance body that considers the ethics of the proposal?
8. Is consent from the original data providers required?
9. What collaboration opportunities could the project provide to improve organisational processes?

In terms of potential information requirements for Safe Projects for CADRE, the CWG identified the following indicators of interest:

- **Intended use**: What is the proposed project to be undertaken using the data? This could include a series of sub-indicators:

    - **Fitness for purpose**: will the data being requested meet the information needs of the project being proposed?

    - **Public benefit**: does the project provide an overall public benefit?

  - **Academic contribution:** will the project being proposed make a contribution to the scholarly academic record?

  - **Commercial benefit:** will commercial benefit be derived from the results of the project?

- **Context**: what is the context under which the project is being undertaken? Is the project a one-off activity or does it constitute part of an ongoing relationship or activity?

- **Ethics:** what are the ethical considerations of the project to be undertaken? This can be reflected in:

  - Has an **ethics application** been completed for the project?

  - Has a **privacy impact assessment** been completed for the project?

  - Are there relevant **codes of conduct / use** surrounding the conduct of the project (e.g., university codes of conduct, or professional standards bodies)?

- **Risks**: What are the forms of risk associated with the project?

  - **Confidentiality risks** for those people or organisations who are represented in the data.

  - **Reputational risks** to the custodian and the user of the data of misuse or misunderstanding of the data.

  - **Commercial risks** of loss of intellectual property and commercial value through misuse of the data.

- **End user** of the project – who is the ultimate end user of the analysis and outputs of the project to be completed. The following are indicative of the end user and the project intent and benefit – and they may all be the same, or varied:

  - Who is the **sponsor** of the research?

  - **Who** is the research being conducted for?

  - **Who is funding** the research?

Relationship to other Safes

Four further themes were considered by the CWG in their analysis of Safe Projects.

- Who is conducting the research?

- What is the data user's institutional status?
- When safety is being considered?
- Whether the project is part of a broader research activity?

Two of these – **who is conducting** the research, and the **institutional status** of the data user - are taken up further in the Safe People section, as the group agreed that they relate more to the person than the project.

The third additional theme related to the question of **when safety is being considered**. This theme was framed in terms of "Safety Before versus Safety After" – focusing on at what point in the life of the data are we assessing safety. Here the group distinguished "Safety Before" as the circumstances under which the data were ***originally collected***, which was assessed as a characteristic of the data (rather than the project). The question of "Safety After" related to how the custodian might assess the safety of the ***project outcomes***. This essentially relates to the End Users and Risks associated with the project, and so is largely incorporated in the to the earlier items. Implied here is consideration of "Safety During" the project i.e., changes to the aims and activities of the project while it is being undertaken.

The fourth theme in the group was the question of how to consider larger **programs** of research activity, of which a project might be only one part. This could be within the context of a long-term research program, or the activities of a single researcher within a larger research centre, or part of student course work. This points to the need to consider aggregations of projects within programs as an additional element of the framework. This need for grouping also occurs with other Safes, and this point is expanded upon in the Limitations and Additional Requirements section.

Safe People

An assessment of a user as a Safe Person involves the question "Can the researchers be trusted to use it in an appropriate manner?". Desai et al (2016) suggest that that this analysis involves a consideration of "the knowledge, skills and incentives of the users to store and use the data appropriately".

Within the data access literature, an assessment of Safe People is largely oriented around user training, with some small consideration of procedures (and penalties for not following them). Ritchie and Green (2020) articulate three questions for an assessment:

- Do the users have the necessary technical skills?
- Do the users need training in handling confidential data?
- Are users likely to follow procedures?

Similarly, the majority of assessment questions that are identified by the ONDC for Safe People relate to their procedural knowledge and training questions (ONDC, 2019).

The training of researchers as data users is well established in the Australian context. The Australian Bureau of Statistics incorporates DataLab safe researcher training as a user requirement before any of their secure data products can be accessed (ABS, 2021). Researcher training has been developed by the ERICA (eResearch Institutional Cloud Architecture) team at the Centre for Big Data Research in Health at the University of New South Wales to prepare and vet researchers that seek to use sensitive data on their research platform (Department of Health, n.d.). These user training programs focus on various issues including user obligations, use of systems, training on specific datasets, and the process and release of outputs from a safe setting environment.

For the CWG however, an additional set of criteria emerged around the idea of a safe person, that related to user experience and institutional context. The group articulated two types of information that would also be reviewed in an assessment:

- **Past track record**: primarily oriented around publication and research history, reflecting both domain knowledge and research training.

- **Institutional affiliation**: oriented around the organisation(s) that the user was associated with undertaking the research to be completed. This characteristic was recognising that an institutional affiliation provides additional forms of support for the use of the data:

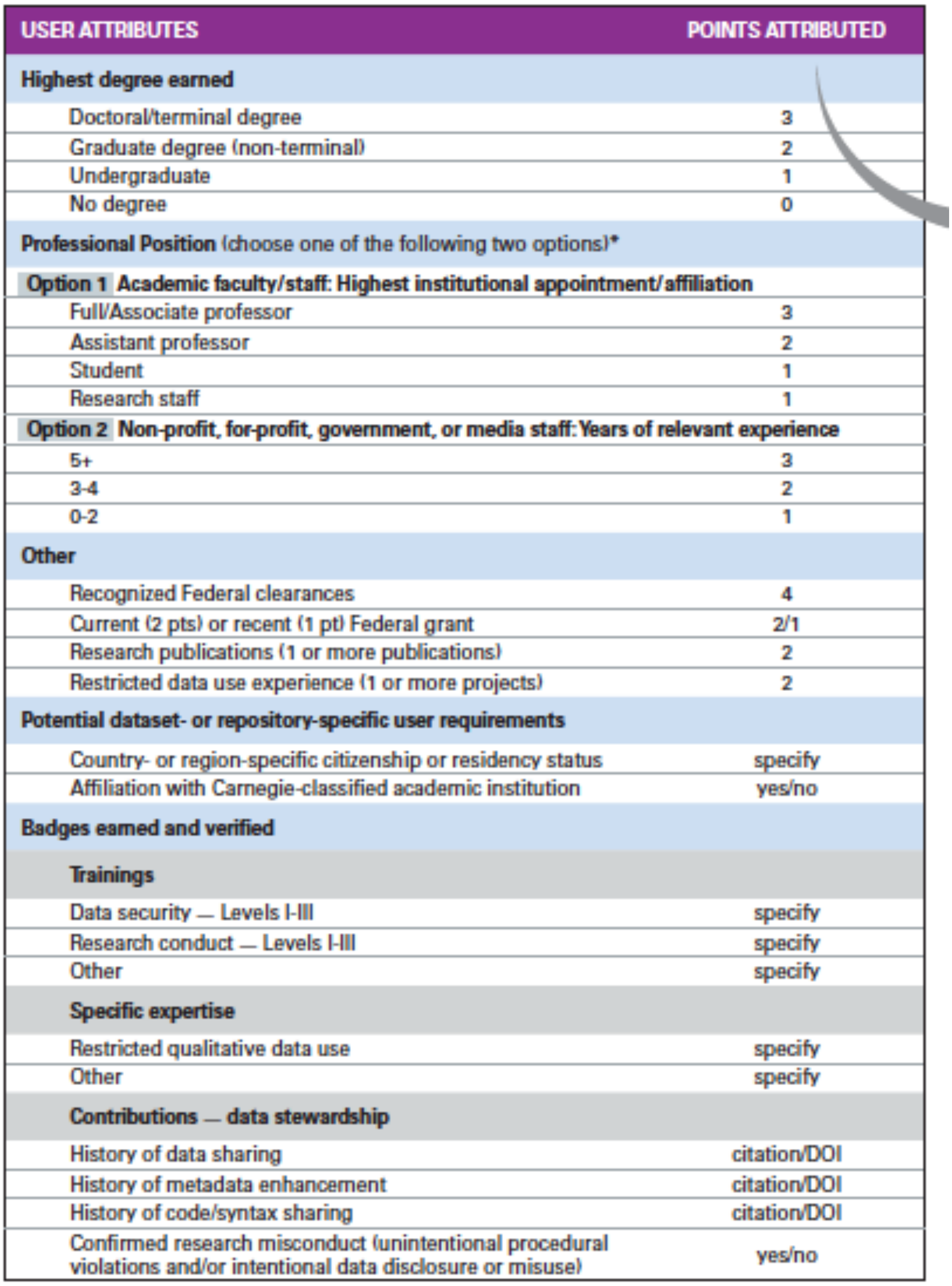
    - **Institutional rules** which provide guidelines and regulation on the activities that the researcher can undertake (such as ethics committees)

    - **Institutional support** in the form of guidelines, training, and researcher support for data use activities, that can ensure a level of procedural knowledge and experience is available or can be developed through supervision (such as higher degree supervision arrangements)

    - **Institutional legitimacy** in terms of public trust as a suitable context in which to use data. There is a clear set of expectations among the public about which institutions they trust to use data effectively and appropriately, that can facilitate the social license to share among data custodians (Biddle et al., 2018)

An approach to addressing these additional criteria has been developed by the Inter-University Consortium for Political and Social Research at the University of Michigan. The “Researcher Passport” system (Levenstein et al., 2018) outlines an approach for researcher credentialling that allows the capture of user attributes progressively, aligned with a related “points” system for the recognition of additional experience. As shown in Figure 1, the ICPSR model outlines possible user attributes and associated rating points that signify levels of professional knowledge (and therefore readiness) for access to sensitive data. A similar concept of the “Researcher Passport” has also been implemented within the genomics community. The Global Alliance for Genomics in Health (GA4GH) has developed a passport management system (GA4GH, 2021a) also entitled a “researcher passport” that enables the transfer of tokenised information about a researcher (GA4GH, 2021c) between institutions to facilitate access to data and settings.

Figure 1 The ICPSR Research Passport User Attributes. (Source: Levenstein et al., 2018, p.21)



USER ATTRIBUTES	POINTS ATTRIBUTED
Highest degree earned	
Doctoral/terminal degree	3
Graduate degree (non-terminal)	2
Undergraduate	1
No degree	0
Professional Position (choose one of the following two options)*	
Option 1 **Academic faculty/staff: Highest institutional appointment/affiliation**	
Full/Associate professor	3
Assistant professor	2
Student	1
Research staff	1
Option 2 **Non-profit, for-profit, government, or media staff: Years of relevant experience**	
5+	3
3-4	2
0-2	1
Other	
Recognized Federal clearances	4
Current (2 pts) or recent (1 pt) Federal grant	2/1
Research publications (1 or more publications)	2
Restricted data use experience (1 or more projects)	2
Potential dataset- or repository-specific user requirements	
Country- or region-specific citizenship or residency status	specify
Affiliation with Carnegie-classified academic institution	yes/no
Badges earned and verified	
Trainings	
Data security — Levels I-III	specify
Research conduct — Levels I-III	specify
Other	specify
Specific expertise	
Restricted qualitative data use	specify
Other	specify
Contributions — data stewardship	
History of data sharing	citation/DOI
History of metadata enhancement	citation/DOI
History of code/syntax sharing	citation/DOI
Confirmed research misconduct (unintentional procedural violations and/or intentional data disclosure or misuse)	yes/no

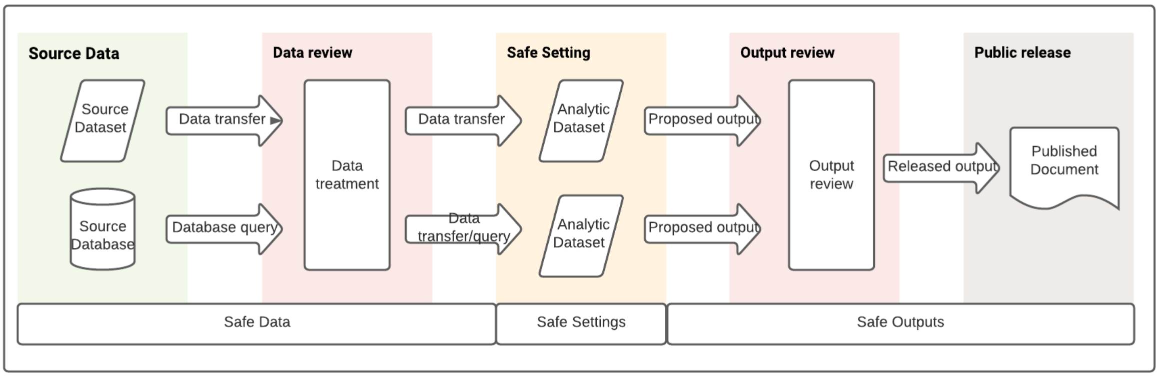
Safe Data

Ascertaining the foundations of safe data involves asking the question “Is there a disclosure risk in the data itself?”. For Desai et al. (2016, p.11) this involves “primarily to the potential for identification in the data… [but] …it could also refer to the sensitivity of the data itself”. The foundation of a safe data evaluation begins with confidentiality considerations, but as noted by ABS, this then also should entail the discussion of the trade-offs between confidentiality and the utility involved in the process of anonymisation (ABS, 2017).

There is an extensive literature on the methods for statistical disclosure control, the field of research associated with the management of data intended for release. Software packages have been developed to assess disclosure risk, including open-source R package *sdcMicro* (Templ et al., 2015) and the μ-ARGUS package developed by the Statistics Netherlands (2021). Additionally, treatments for disclosure risks are broadly available, such as the *De-identification Decision-making Framework* developed by Data61/CSIRO (O’Keefe et al., 2017), and the *Handbook on Statistical Disclosure Control for Outputs* (Griffiths et al., 2019) developed by the Secure Data Access Professionals community of practice (UKDA, n.d.) of data access managers in the United Kingdom.

It should be noted that statistical disclosure control assessments are also applied to Safe Outputs released from Safe Settings such as research data centres and remote processing environments. In this section of the framework, we consider treatments applied prior to the release of data into a Safe Setting, whereas Safe Output assessment occurs at the point of release out of the Safe Setting. Ritchie and Green (2020) refer to the former as “input statistical disclosure control” and the latter as “output statistical disclosure control”. This distinction is considered further in the discussion of Safe Outputs and reflected in Figure 2.

Figure 2 Safe Data, Safe Settings and Safe Outputs



The question of whether data treatments are suitable and effective in managing disclosure risks is an area of active research. As noted elsewhere, researchers in cryptography have demonstrated that some treatment processes can be effectively reversed given the prevalence of publicly available information through the internet (Culnane et al., 2017). Culnane and colleagues (Culnane et al., 2020) also provided a critique of the Five Safes framework more generally. A related paradigm of differential privacy (Garfinkel et al., 2019) is aimed at addressing concerns raised within this domain, including the forthcoming release of the 2020 United States Census, but this approach brings with it a different set of challenges, particularly around fitness for use (Ruggles et al., 2019). For now, the mechanisms of statistical disclosure control are the predominant method of assessment and intervention for practical reasons, particularly when considered jointly with an application of the remaining four Safes in the Five Safes framework.

There are also some questions around the use of disclosure risk assessment techniques as a suitable method for determining access to qualitative social science data. There is a significant difference in the nature of disclosure risk when assessing quantitative and qualitative data (McLeod et al., 2020). A higher risk of both direct and indirect breach of confidentiality can occur with access to qualitative data (Corti et al., 2000; QDR Study, n.d.; Kirilova & Karcher, 2017).

An illustration of these risks was in the major data archiving project completed by the SOCEY team across multiple qualitative data collections (see McLeod et al., 2020). This work highlighted the difficulties associated with anonymisation of qualitative data, which concern the importance of retaining contextual detail, the time-consuming nature of manual anonymisation and the limitations of automated anonymisation software. It also highlighted that confidentiality is not an inherent requirement in all cases – there are situations where the participant consents to be identified – yet these still need to be managed carefully to protect participant data from misuse. This work suggests that "Safe Data" may not be possible for some qualitative collections – therefore necessitating the stronger emphasis on the other "Safes" for enabling access.

Beyond the question of statistical disclosure and utility, the CWG identified a series of additional considerations in the assessment of "Safe Data". These additional questions were associated with three broad areas – (1) the **usability** of the data, (2) **integrity** of the data and contextual information, and (3) the **access conditions** associated with the data.

Regarding **usability of the data**, the CWG pointed to the need for contextual information (often metadata or paradata) that could better support use – that is, enabling the data to be appropriately and thus safely used. This could include:

- Provision of multiple forms of the data, such as the General and Restricted Releases of the longitudinal datasets from the National Centre for Longitudinal Data.

- Availability of structural and contextual metadata (such as data dictionaries, project descriptions and context statements).

- Availability of "test" or synthetic versions of the data, which can be used to test procedures prior to access to the actual release data.

In terms of **data integrity**, the group identified the following considerations:

- The need for contextual information to enable understanding of some (or even all) collections.

- Whether some data should in fact be treated – that it may be inherently destructive to the use of the data to provide a treatment.

- The potential need for a curatorial process to assess suitability for treatment or anonymisation that is field specific and requires training relevant to that field.

The third area – **access conditions** – was the subject of some discussion. Access conditions specify the constraints that the data custodian places on the data as a condition of their use. It can include a specification of preferred options for the other safes, such as:

- User characteristics e.g., access for staff but not students
- Limits on purposes e.g., no use for commercial purposes
- Time-limited access to data or work environment (as resources)
- Notification on and review of outputs from analysis of the data
- Licenses and other documentation required

The agreed position of the CWG was however that access conditions are ideally attributes of the data (or the data collection) – that they are specifications under which a data collection may be made accessible. The intent then is that the data custodian (or their agent, such as the Australian Data Archive) can ideally streamline the data access process by aligning the collection of information about the details of other "Safes" (e.g., the attributes of the Safe Person) and then making a comparison of that information about the user with the access conditions in support of use (or not).

Safe Settings

Within the Five Safes framework, the concept of safe settings relates to the setting or environment in which the data is being accessed – that is, the physical, technical and informational context of the data access. The core question to be addressed of a safe setting is "Does the access facility limit unauthorised use?" (Desai et al., 2016).

The Office of the National Data Commissioner (2019) describes an assessment of safe settings as follows: "whether all parties have taken reasonable steps to ensure data will be used in an appropriately safe and secure environment i.e., one that minimises unauthorised use, access or loss of data" (ONDC, 2019, p.20). They distinguish two core areas – the physical environment of the data access, and the IT environment. Notably, the ONDC also reference training of users in relation to these environments, highlighting the interaction of the Five Safes dimensions - Safe People with suitable training and knowledge are a key element in the effective operation of a Safe Setting.

Government agencies and data infrastructure providers have a long history in the provision of safe settings for academic research activities. An overview of the range of options, along with the associated data accessible through each option, was originally identified as the Data Access Continuum (Goldmann, 2009/10), a predecessor of the Five Safe models (Ritchie, 2017), The Data Access continuum has been applied in a number of countries, including Australia, Canada and the United Kingdom (Goldmann, 2009/10; Desai et al., 2016; Tam et al., 2009).

Ritchie and Green (2016) also reviewed the available options for the Commonwealth Department of Social Services in a study of data access options for longitudinal studies. They identified the four core options for access environments (with several variations on the third option of distributed analysis), detailed in Table 2.

Table 2 Data Access Settings classification (Source: Ritchie and Green, 2016)

Access setting	**Description**
1. Secure on-site research facilities (research data centres or RDCs)	A secure physical facility with access requiring the user to be in the same physical place as the data, in a facility controlled by the data owner.
2. Distributed data (licensing)	Sending data to users via open or encrypted data files
3. Distributed analysis, broken down into:	
(a) Remote tabulation	Software tools designed to allow users to create their own tabulations of the data
(b) Remote job servers	Tools enabling users to submit code to a server which runs the code on the data and generates results
(c) Remote or virtual RDCs	Remote desktop environments allowing users to operate software, conduct analysis and see data in a virtualised environment
(d) Analysis services	Serviced research requests where researchers develop code for execution. This is sent to the data owner, who execute code, check outputs, and return results
4. Synthetic data	Creation of imputed data that is sufficiently ‘close’ to the original data to allow for valid analysis, but without the confidentiality risk

Recent developments in other domains, notably in biosciences, have provided similar classifications. As part of the bioCADDIE Project (n.d.) funded by the US National Institutes of Health, a team of researchers have worked to establish the Data Tags Suite (DATS). DATS, a metadata schema for “describing data access, data use conditions, and consent information” (Alter et al., 2020) has five levels of classification (Table 3).

Table 3 Data Tags Suits (DATS) Descriptors for Access (Source: Alter et al., 2020)

Access method	**Description**
Download	The data are available for download. A license may be required
API	Interaction with the data may be automated via defined communication protocols, i.e., APIs
Remote access	Users may access the data in a secure remote environment (“virtual data enclave”). Individual-level data may not be downloaded, only approved results

Access method	Description
Remote service	A user may submit program code or the script for a software package to be executed in a secure data center. The remote site returns outputs. It may perform a review before releasing the results
Enclave	Access is provided to approved users within a secure facility without remote access. Results may remain at the enclave or be released after review

The classification provided by Ritchie and Green is useful for delineating existing services, and CADRE project partners and stakeholders involved in delivery of Safe Settings can be classified across these four options (Table 4). For example, the Australian Institute of Health and Welfare profile their service offerings across different access environments (AIHW, 2021).

Table 4 A classification of Safe Settings (Source: Ritchie and Green, 2016)

Setting	Implementation
1. Secure on-site research facilities (research data centres or RDCs)	Australian Institute of Health and Welfare Australian Data Archive (to be certified) Australian Bureau of Statistics
2. Distributed data (licensing)	Australian Data Archive Australian Institute of Health and Welfare
3. Distributed analysis, broken down into:	
(a) Remote tabulation	Australian Bureau of Statistics AURIN *Data CO-OP (TBC)*
(b) Remote job servers	None (formerly ABS)
(c) Remote or virtual RDCs	Australian Institute of Health and Welfare University of New South Wales - ERICA AARNet
(d) Analysis services	Australian Institute of Health and Welfare Australian Institute of Family Studies
4. Synthetic data	Australian Data Archive (1 only) *Other partners (TBC)*

The classification provided by Ritchie and Green does however have limitations, largely a result of significant advancement in the adoption of API services for data access in the intervening period between the two studies. As such, services that might previously been delivered only by a UI-based software tool (such as the ABS Table Builder) are increasingly being replaced by API-based services. Graphical user interfaces are often then being developed to call the API services to generate remote tabulation outputs (such as the Australian Bureau of Statistics ABS.Stat service).

Given the intervening time, the Ritchie and Green and DATS classifications do have a large degree of alignment, partly a result of the common experiences of the two communities. A mapping of the two classifications is presented in Table 5.

Table 5 Comparison of Ritchie and Green (2016) and DATS data access classifications

Ritchie and Green (2016)	**DATS (Alter et al., 2020)**
Secure on-site research facilities (research data centres or RDCs)	Enclave
Distributed data (licensing)	Download
Distributed analysis broken down into:	
Remote tabulation	Remote service (partial)
Remote job servers	Remote service (partial)
Remote or virtual RDCs	Remote access
Analysis services	**No direct equivalent**
Synthetic data	**No direct equivalent** (although synthetic datasets are often accessed through Download)
No direct equivalent	API

For the purposes of CADRE, the DATS classification has the additional benefit of being incorporated into a broader set of web-oriented frameworks, such as the Data Use Ontology and the Open Digital Rights Language – a topic dealt with in the Community Requirements section. One question to be considered is the extent to which the DATS framework might be extended to incorporate the more detailed options for distributed analysis that Ritchie and Green identify, or alternatively whether the "Download" and "API" classifications adequately capture the current range of distributed analysis services available within CADRE partners or elsewhere.

Safe Output

The dimension of safe outputs asks the question "Are the statistical results non-disclosive?" (Desai et al., 2016). The safety of outputs can be considered as "the residual risk in publications from sensitive data" – that is, the risk that is associated with publishing the outcomes of research completed using sensitive data, rather than the risk in the data during its use. The focus of this assessment is on the content that is generated within Safe Settings to produce external artefacts – publications, reports, datasets, results, etc.

There is a distinction that needs to be made between the considerations required for Safe Data, relative to those of Safe Outputs. The Office of the National Data Commissioner outline this distinction in their Best Practice Guide (ONDC, 2019, p.23):

> *The Data Principle applies controls (such as removing direct identifiers and other confidentiality treatments) to the whole dataset available to the*

> *user, whereas the Output Principle applies controls to results that are to be made public or available for further sharing by the authorised user. The Data Principle protects data going from the data custodian to the data user. The Output Principle protects the data subsequent to leaving the data user.*

The practical application of the Safe Outputs principle is dependent on the Safe Setting that is used for access to the data – that is, Safe Outputs assessments are dependent on Safe Settings. The particular limitation lies in the use of download access methods. Once data is downloaded, the data custodian has no opportunity to review any outputs resulting from the use of the data, as there is no process available for enabling the review of the output prior to publication of any results. Desai et al. (2016) note that custodians utilising download methods can incorporate expectations or licensing requirements on the data user to act appropriately, but these requirements are difficult to police in practice.

Vetting occurs as part of the output release, where restrictions are placed on the Safe Setting, either through technical means (such as export/download restrictions from the Safe Setting) or agreed licensing arrangements. In recent years, there has been an emergent set of practices developing for the review of outputs prior to their release. There are two broad approaches to the vetting process, known as principles-based and rules-based output disclosure control.

The application of rules-based disclosure control involves the use of thresholds or deterministic rules to assess outputs as the basis for release or restriction (Griffiths et al., 2019; ONDC, 2019). This can include requirements such as minimum cell counts or restrictions on particularly forms of outputs. While these rules can be (and have been) encoded in automated tools such as the ABS TableBuilder (ABS, 2013), the more common approach is the manual review by a trained output reviewer. One of the aims of the *Handbook on Statistical Disclosure Control for Outputs* was to provide a guide for reviewers. As noted early in the Handbook (Griffiths et al., 2019, p.12), one aim is to:

> *to translate disclosure control concepts into practical advice, measures and steps for assessing statistical results for disclosure risk*

Ritchie and Elliott (2015) identify three core problems of rules-based approaches:

1. No rules can guarantee disclosure
2. A rules-based approach tends to over-protect the data
3. Rules cannot cover all conditions

The challenges in the practical implementation of a rules-based approach led to the emergence of a more discretionary approach, that recognises both practicality in output release and the complexity of many analyses. Known as a principles-based output statistical disclosure control (PBOSDC – Ritchie and Elliott, 2015), this approach relaxes the hard and fast application of rules, to provide guidance to output reviewers through rules of thumb.

The basic characteristics of this approach as outlined by Ritchie and Elliott (2015) are included in Table 6 below.

Table 6 Characteristics of a principles-based output statistical disclosure control (Source: Ritchie and Elliott, 2015)

Researchers and output checkers both trained in SDC
Rules-of-thumb rather than hard rules
Freedom to approve any output in principle
No duty to release any output
Responsibility for producing good output resting with the researcher
Output checkers considering the value of the output
Output checkers considering resource constraints

The principles-based approach is now well-established and recognised by organisations such as the Office of the National Data Commissioner (ONDC, 2019), the Australian Bureau of Statistics (Parker, 2017), and EuroStat, the pan-European statistical agency (Bond et al., 2013).

There is however a recognition in each of these contexts that the principles-based approach also requires an investment in training, both of output checkers and users. This training is designed to facilitate both understanding of the principles and to efficient production and review of outputs. Ritchie et al. (2017) provide useful guidance on elements to incorporate into training programs to prioritise these requirements.

Extensions to the Five Safes

The Five Safes included in the framework are intended as a reference model to consider the various risks associated with the sharing of sensitive data. In considering the application of the Five Safes, both among the Content Working Group and in the experience of project partners, it became apparent that there were additional information areas that are not well represented within the Five Safes. While there may be others, the two areas that were identified in scoping discussions were a specified assessment of organisations, and means for the management of groups.

Organisations

While the Five Safes framework includes a major role for Safe People, it does not explicitly incorporate organisations into the framework. The Content Working Group recognised this as a potential gap in the framework, given the emphasis given to organisational context and affiliations in risk assessments. The reasons for this appear to be three-fold:

1. Organisations can have a **legal status** which can facilitate contracting or other agreement-making (ONDC, 2020b).
2. Organisations provide **resources and infrastructure** that the individual researcher or user relies upon for the conduct of their research (such as technical standards and support services for Safe Settings) (ISO, n.d.; CAUDIT, 2019).

3. Organisational assert **legal and ethical controls** over their affiliated staff, students and associates (such as employment contracts, ethics committees and codes of practice) which provide additional safeguards for the data owner (Alter et al., 2021).

A specific role for organisations is usually implicit, and often explicit, in many data sharing arrangements. In the Australian context, an individual often requires employment or affiliation with an organisation in order to gain access to a data sharing program. For example, access to various sensitive data products through the Australian Bureau of Statistics is managed through organisational subscriptions (ABS, 2021). The *Data Access and Transparency Bill 2020* includes an explicit requirement for organisational affiliation, and a proposed accreditation framework recommending that “An individual may only be endorsed if they are employed by, or acting on behalf of, the accredited organisation and are bound by that organisation’s policies and procedures.” (ONDC, 2020b). The ICPSR Researcher Passport attributes also include an institutional affiliation (using the US Carnegie classification) as an optional requirement for access to specific datasets, an access condition that is at the determination of the data owner.

While these schemes may not necessarily exclude individual independent researchers who do not have an organisational affiliation, such individuals are likely to incur additional transaction costs in demonstrating their need for such services. The ONDC (2020b) provides the example of accreditation for the independent researcher in their discussion paper, but notes that a researcher will still need endorsement of their accreditation by an organisation.

Groups

The second key characteristic not present in the Five Safes framework is the recognition of a role for groups, and associations of each of the Safes. The most obvious of these grouping characteristics is the association of a person within an organisation, and the characteristics of organisations are considered above, but there are however other natural groupings that occur.

Examples of possible grouping requirements for the management of data sharing activities are presented in Table 7. Some of these groupings may more abstract than the formal Five Safes considered so far, but others (such as Research Teams) are often required to be explicitly specified in data access requests.

Table 7 Examples of Groups of Safes

Five Safes dimension	**Grouping**
Safe People	**People** working in **Research teams**
Safe Projects	**Projects** completed as part of larger **Work Programs**
Safe Data	A **Linked Dataset** resulting from linkage or integration of **multiple upstream Datasets**

Five Safes dimension	**Grouping**
Safe Settings	Use of **Data** from multiple sources located in **multiple Settings** (and the need for coordination between settings, to enable suitable ingress and egress under controlled conditions)
Safe Outputs	**Multiple publication Outputs** resulting from a completed analysis

The Content Working Group gave consideration to the role of grouping in different circumstances. While "Safe Groups" were not seen as an additional requirement to the Five Safes, the need for a mechanism for organising groups was recognised as a key requirement, to enable the explicit linkage of different groups of Safe attributes within data access management processes.

The "Joint and Several" Application of the Five Safes

As noted earlier, the Five Safes is intended to operate both severally and jointly – each Safe can be separately assessed ("severally"), but the overall application of the framework should take into consideration the full range of Safes concepts and options being proposed in a data sharing arrangement or model ("jointly"). To this end, there are several key intersections and alignments that have been identified by the Content Working Group requiring additional extrapolation.

Key Intersections

The preceding discussion of each of the Five Safes has identified several intersections where two or more Safes tend to be considered in parallel in the assessment of risk. A summary of these intersections is included in Table 8.

Table 8 Key information intersections in CADRE framework

Intersection	**Example**	**People**	**Projects**	**Data**	**Settings**	**Outputs**
People and Projects	Data custodians assess the characteristics of the person (such as the type of organisation they work in) in assessing the project.[1]	▨	▨			
Projects and data	Data custodians will assess the project requirements and research questions in determining the content of the dataset to make available for the project.		▨	▨		
Data and Settings	A data provider will assess the setting and how the data will be accessed in determining what level of treatment to			▨	▨	

[1] If a researcher is working in a *for-profit* company conducting research that is primarily for public benefit are the benefits largely private or public?

Intersection	Example	People	Projects	Data	Settings	Outputs
	apply to the data prior to transferring it to the setting.			■	■	
Settings and outputs	A data custodian will assess the capacity of the setting to allow review of the outputs in assessing its suitability for use.				■	■
People and settings	Users of settings are required to undertake training in the Five Safes and the specific setting before access to the setting is provided.	■			■	
People and outputs	Researchers using settings are trained in suitable outputs for release as part of training programs – a "virtuous circle" model (Ritchie et al., 2017).	■				■

Key Alignments

Through the process of review and engagement with the Content Working Group, a number of key alignments for information requirements for each Safe have been identified. These alignments have been identified in Table 9.

Table 9 Key information alignments in CADRE framework

Alignment	People	Projects	Data	Settings	Outputs
A researcher's roles and their organisational affiliation e.g., post-grad student or professor and research assistant or chief investigator.	■	■			
Data custodian's assessment of suitability of data treatments depends on the setting it will be available in, and whether additional output check will (or can) be undertaken.			■	■	■
Data custodian's assessment whether an intended user (a researcher) has undertaken suitable training (e.g., for a given dataset, for use of a given setting, in production of outputs).	■		■	■	■

Limitations and Additional Requirements

While the CADRE framework seeks to incorporate a broad range of interests and use cases, there are some scope limitations that have been identified that CADRE will not address until later releases. Some of these future requirements and limitations are included below:

- The conceptualisation of the framework has been developed with the ONDC DataPlace as a service to interoperate with in the future. As the DataPlace development moves to engagement with higher education around accreditation and the management of researcher access to government in federal agencies, the emergence of Accredited Data Service Providers and organisational research policies instituted will have an impact on this conceptualisation of the Five Safes.
- It is anticipated that the four themes outlined in the Relationships to other Safes section will need to be revisited to understand the impact of time on concepts of safety i.e., safety before, during and after a research project and the effects of iteration of research i.e., how projects and programs are related to ongoing data access requests.
- An extension of the requirements analysis (beyond that of social science and health) to another allied domain e.g., humanities it is anticipated would enable some consideration of geo-spatial, jurisdiction and cultural considerations.
- The Five Safes framework does not encompass cultural safety protocols and concepts articulated in Indigenous Australian knowledge systems. A review of the CADRE Five Safes framework in context of the AIATSIS code of ethics (AIATSIS, 2020) and expert input from Indigenous Data Network (n.d.) representatives is needed.

Five Safes – Operationalisation

The CADRE Platform will be a shared and distributed sensitive data access management platform for the social sciences and related disciplines. The operational model established draws directly from the Five Safes framework and will enable data owners and users to address core concerns around data governance, creation, management and sharing of sensitive data for research.

Community Requirements

Common Requirements

CADRE informatics and analytics are determined through capture of common information requirements from project partners around managing data access requests and providing research environments that draw upon the Five Safes framework for risk assessment. The objective in establishing the CADRE information exchange is to replace multiple documents and web forms, provide a common interface to capture information (using shared terminology, information standards and extensibility principles for local variation) as a decision-support system. An information model that underpins the information exchange is in development based on the shared requirements around sensitive data access requests and the chain of custody associated with data, as data (and researchers) move across systems.

Information Exchange

The CADRE platform project includes the development of an information exchange where metadata is supplied by a data requestor and drawn in from multiple sources. An information model is proposed as a means to capture relevant information and streamline researcher requests for access to sensitive data. The CADRE conceptual framework (drawing upon the Five Safes framework)

There are three ordered questions (information sought and received) that lead to an access request being satisfied or rejected.

1. **Person & Affiliation**: Who is asking for this data and what is their affiliation?
2. **Data & Request**: What data is being sought and what do they intend to do with it?
3. **Authorisation & Access**: What authorisation is suitable and how is access enabled?

Information Model

The CADRE information model in development is based on high-level requirements provided by the project partners:

- CADRE entity relationship diagram – for information exchange v0.2
- CADRE business architecture v0.1
- CADRE technical architecture v0.1
- CADRE metadata flow v0.1

Authentication and Identity Assurance Framework

At the heart of the CADRE information model lies the authentication and identity assurance framework in development by the Australian Access Federation.

The evaluation, selection and implementation of standards to support the "Safe People" aspect of the Five Safes framework is a critical first step in enabling management of secure access to data within the Australian research environment. In particular the agreed attributes and identifiers that are associated with people, organisations and groups (and as appropriate for other dimensions of the Five Safes) – that are provided by members of the Access Federation as assertions.

Establishing whether a data requestor is a "Safe Person" is the starting point for a sensitive data access request and first order questions are to ascertain a person's identity, their affiliations and roles.

Scope for the information model (this version) is:

- Guidance provided by the CADRE conceptual framework (to operationalise the Five Safes)
- Information (metadata) exchange as part of the decision-support mechanism for sensitive data access requests
- Disambiguation and harmonisation processes provided by Research Graph for enriching scholarly metadata (Augment API)
- Access request management including request, authorisation, project and group metadata that can be linked to data descriptions and identity verification
- Metadata that can be passed between systems integrated with the information (metadata) exchange is based on overlapping requirements from the four settings
- Interoperation (metadata exchange) with the four settings and the AAF and Research Graph attributes

Out of scope (for this version)

- Research accreditation information
- Interoperation with DataPlace development
- Interoperation with Accredited Data Service Providers
- Automation of data supply as a result of a successful sensitive data access request

Scope for documentation (this version)

- Metadata sources i.e., institutional, safe setting, identifier service, public web
- Metadata semantic areas, standards, known or potential attributes, types/categories
- Metadata prioritisation and conceptual linkages that support decision-making
- Minimum viable metadata set for multi-system use i.e., semantics and identifiers
- Relevant "Safes" from the CADRE conceptual framework (drawing from Five Safes)

Semantic areas to cover in the information model:

- Person & Affiliation
- Data
- Request
  - Project
  - Group
- Authorisation
- Access

The CADRE information model is shaped by the conceptualisation of the Five Safes and requirements captured, and in turn shapes the data model developed to operationalise the Five Safes.

CADRE Data Model

Information to support access sensitive data access request administration and secure data management and the attributes to form the shared data model are summarised. Technical protocols and assertions made by members of the Australian Access Federation will play a key role in prioritising information for risk assessment as part of decision-support.

CADRE Data Model	
Person & Affiliation • Display Name • Family Name • Full Name • Given Name • Researcher ID / ORCID • User Email • User Name • Affiliation • Affiliation ID / ROR • Affiliation Role / (AAF)	Request (Activity) • Activity Name • Activity Description • Activity ID / RAID, Local ID • Activity Role / Local • Activity Dates / from, to • Request ID / Local ID • Funding ID / ARC, NH&MRC • Ethics Reference No.
Data • Data Name • Data ID / DOI, handle • Use Requirements / (DUO) • Publication ID / DOI	Request (Group) • Group Members • Group Name • Group Entitlements • Group Dates / from, to
Authorisation • Authorisation Source • Authorisation ID / Local ID • Authorisation Entitlements / Local, jurisdiction, geo-spatial • Authorisation Dates / from, to	Access • Service Provider / CADRE settings • Access Path / (AAF) • Access Type / [DATS]

Domain Requirements

Frameworks for standardising sensitive data access processes are reflective of the particular sensitivity and safety constraints associated with the data used and research undertaken in that sphere. Efforts to harmonise data use, data access and authorisation processes have been an area of increased focus, both within the social sciences, and in other domains with sensitive data management requirements. Two frameworks in this area from the genomics and life sciences domain are of particular note and considered in detail – the Data Use Ontology (2021) used by the European Genome-Phenome Archive and the Broad Institute, and the Data Tags Suite (Sansone et al., 2017; Alter et al., 2020).

Analysis of the frameworks is undertaken to assess whether these frameworks may be a means for specifying business rules for the CADRE information exchange. These business rules would be based on the requirements gathered from the CADRE partners working in social science and health research and/or serve as a means to more effectively broker access to sensitive data and manage research environments. In particular efforts to standardise data use controls Automated Data Access Matrix (ADA-M) to define a matrix of data use categories by Global Alliance for Genomics and Health (GA4GH) that assist with managing use restrictions and biomedical research purposes (Woolley et al., 2018). Interoperability and scalability are also major considerations to ensure both fit for social science and flexibility to accommodate allied domains, and sustainability. The disciplinary clusters developed as part of the European Open Science Cloud are global exemplars (Hasani-Mavriqi et al., 2020)

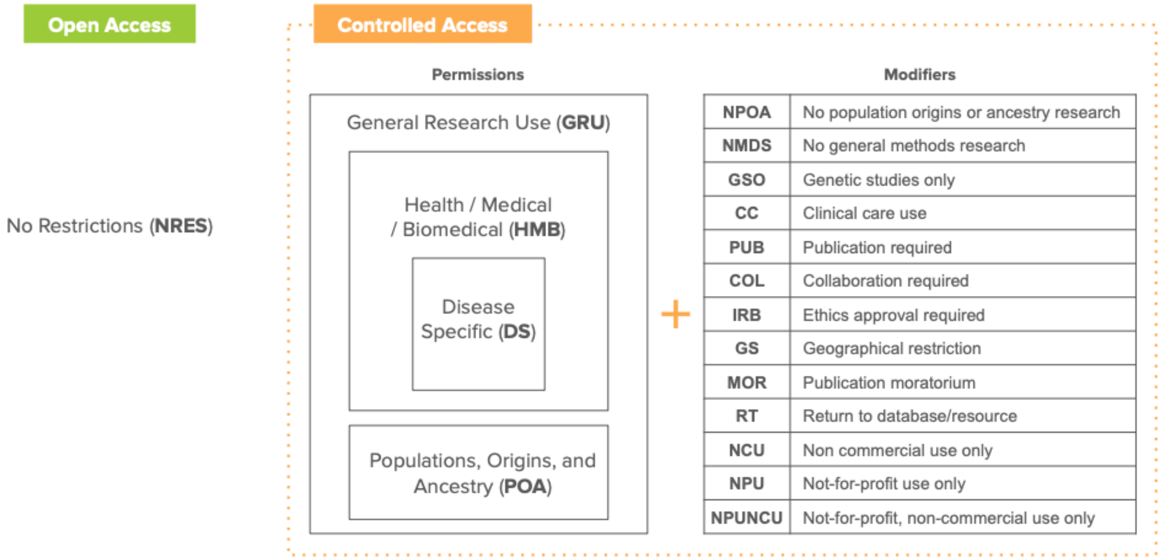
> *The technical interoperability of research infrastructures was identified as another crucial challenge. Semantic interoperability, … to focus more on the balance between general, cross-discipline and discipline specific solutions and standards. The European Open Science Cloud (EOSC) was mentioned as an exemplar of the latter.*

Data Use Ontology (DUO)

The Data Use Ontology (2021a) was established by the GA4GH to enable data providers to "semantically tag genomic data sets with data use information (such as restrictions on use and modifiers). DUO is used in genomics archives in the USA and Europe to provide automated discovery of usage terms, and progressively to automate the data access and approvals process.

The intent of DUO is to establish a foundation of data use permissions or limitations (DUL) and usage modifiers (see
Figure 3). The combination of the core permissions and modifiers allow for the semantic tagging of datasets with categorised usage restrictions. This information can then be used as a basis for search across collections, allowing users to limit their search to data that is accessible to them, and consistent with their research activities and requirements.

Figure 3 Data Use Permissions and Modifiers (Source: Courtet, 2021; Credit: Stephanie Li, GA4GH)


Open Access
Controlled Access
Permissions
Modifiers
No Restrictions (NRES)
General Research Use (GRU)
Health / Medical / Biomedical (HMB)
Disease Specific (DS)
Populations, Origins, and Ancestry (POA)
+
NPOA No population origins or ancestry research
NMDS No general methods research
GSO Genetic studies only
CC Clinical care use
PUB Publication required
COL Collaboration required
IRB Ethics approval required
GS Geographical restriction
MOR Publication moratorium
RT Return to database/resource
NCU Non commercial use only
NPU Not-for-profit use only
NPUNCU Not-for-profit, non-commercial use only

The tagging of data use restrictions is also intended to enable the streamlining of data access request processes based on such conditions. Members of the GA4GH community have now incorporated the DUO tags into their data access management systems, including the Broad Institute's "Data Use Oversight System" and the European Genome-Phenome Archive.

How then might CADRE make use of the DUO framework? In the first instance, elements of the DUO framework align readily with the Safe People, Projects and Outputs dimensions outlined in the Framework Structure section. Table 10 provides an initial classification of each of the DUO permissions and modifiers against the Five Safes framework based on the DUO ontology (DUO, 2021b).

Table 10 Mapping of DUO tagging to the Five Safes

Five Safes dimension	**DUO permissions**	**DUO modifiers**
(Non-specific)	NRES - No Restrictions	
People		GS – Geographical restriction COL – Collaboration required US – User specific restriction
(Organisations)		Institution specific restriction NPUNCU – Not-for-profit, non-commercial use only*
Projects	General Research Use (GRU) Health/Medical/Biomedical (HMB) Disease specific (DS)	NPOA – No population origins or ancestry research NMDS - No general methods research GSO – Genetic studies only

Five Safes dimension	**DUO permissions**	**DUO modifiers**
(Non-specific)	NRES - No Restrictions	
	Populations, Origins, and Ancestry (POA)	CC – Clinical care use IRB – Ethics approval required NCU – Non-commercial use only NPU – Not-for-profit use only NPUNCU – Not-for-profit, non-commercial use only* PS - Project specific restriction TS - Time limit on use
Data	*(None)*	*(None)*
Settings	*(None)*	*(None)*
Outputs		PUB – Publication required MOR – Publication moratorium RT – Return to database/resource

Application of the DUO tagging could then be applied at different points in the CADRE data access process to align data custodian requirements with user request processes.

Australian Data Archive Examples

Consider two datasets in the ADA collection – the *Australian Survey of Social Attitude*s (McNeil et al., 2021) and the *Longitudinal Survey of Australian Youth* (Department of Education, Skills and Employment, 2021). These datasets have differential requirements for the type of project that they can be used for (Safe Project), and which users are allowed to use the data (Safe People/Organisations).

Table 11 presents an overview of how these two datasets would be tagged. This tagging could then be used as both a filtering mechanism as part of the search of ADA data collections, and then in the set of specific content requirements included in a data request process. These content requirements could be captured through either existing information available through CADRE (such as the non-profit status of an organisation) or new questions included in a request form – which can then be made available through CADRE for use in other data requests.

Table 11 Example tagging of Australian Data Archive datasets with DUO metadata

Australian Survey of Social Attitudes DOI: 10.26193/C86EZG	**Longitudinal Survey of Australian Youth** DOI: 10.4225/87/PJO7GB
Data Use Limitations – DUO tags	
GRU - General Research Use - DUO_0000042	GRU - General Research Use - DUO_0000042
Modifiers – DUO tags	
PS - Project specific restriction – DUO_0000027	PS - Project specific restriction – DUO_0000027 GS - Geographic restriction – DUO_0000022

The DUO ontology has two limitations in terms of its applicability for social science sensitive data.

The first of these limitations is a result of its orientation towards genomics and health research. Applications in the social sciences, humanities and arts would need to incorporate both limitations and research purposes that are consistent with applications in these domains. That said, a reasonable proportion of the content of DUO does however map relatively clearly to humanities, arts and social science (HASS) datasets, and with suitable extensions could be readily developed under the DUO “Data Use Permissions”, with a branch of “Social Science and Humanities research” uses parallel to the current “Health or medical or biomedical research” hierarchy (DUO, 2021c).

The second limitation for DUO is in the extent of its coverage of the Five Safes. The mapping of DUO and the Five Safes in Table 10 demonstrates that DUO does not cover aspects of either Safe Data or Safe Settings. For this reason, it is necessary to consider a second framework, the Data Tags Suite.

Data Tags Suite (DATS)

The Data Tags Suite (DATS) was established with the aim to provide better support for data access conditions in datasets. The suite, an outcome of the bioCADDIE project run by the US National Institutes of Health, was developed to support data searching across biomedical collections, and align user search and access activity with the requirements of data custodians, to facilitate the establishment of the data use agreements prior to release of data to users.

The focus of DATS is to facilitate the process of finding and accessing data (consistent with the FAIR principles). DATS highlights three core activities in this process:

- ***Authorisation***: “obtaining permission from the party that owns or is responsible for protecting the data”
- ***Authentication***: the requirement for “some kind of login process to identify the user”

- ***Access***: the environment or setting in which the user is allowed to gain access to the data

Alter et al. (2020) provide a set of descriptors for each of the three A's (Authorisation, Authentication and Access) included in Table 12, Table 13, and Table 14. The Access descriptors summarised earlier in Table 3 (in the discussion of Safe Settings) and are reproduced here for context.

Table 12 Descriptors for Data Authorisation (Source: Alter et al., 2020)

Authorisation type	**Description**
None	Not covered by a DUA.
"Click through" online license	Users must agree to an online agreement without providing additional identification.
Registration	Users must register before access is allowed and agree to conditions of use. Registration information may be verified.
DUA signed by an individual	An agreement signed by the investigator is required. DUAs may require additional information, such as a research plan and an IRB review (see discussion of licenses below)
DUA signed by an institution	An agreement signed by the investigator's institution is required. DUAs require additional information, such as a research plan and an IRB review (see discussion of licenses below)

Table 13 Descriptors for Data Authentication (Source: Alter et al., 2020)

Authentication type	**Description**
None	No authentication required.
Simple login	Single-factor login or the use of an authentication key or registered IP address is required.
Multi-factor login	Multiple-factor login using a combination of IP address, password protection, authentication key, or other forms of authentication.

Table 14 Descriptors for Data Access (Source: Alter et al., 2020)

Access method	**Description**
Download	The data are available for download. A license may be required.
API	Interaction with the data may be automated via defined communication protocols, i.e., APIs.
Remote access	Users may access the data in a secure remote environment ("virtual data enclave"). Individual-level data may not be downloaded, only approved results.

Access method	Description
Remote service	A user may submit program code or the script for a software package to be executed in a secure data center. The remote site returns outputs. It may perform a review before releasing the results.
Enclave	Access is provided to approved users within a secure facility without remote access. Results may remain at the enclave or be released after review.

The value of the DATS framework for CADRE is in two areas.

Firstly, DATS provides the capacity for data custodians to specify a light-touch characterisation of the Safe Settings requirements for access to data in their control, through the combination of Authorisation and Access descriptors. For example, the Australian Data Archive's Open, General and Special Release models have been classified (ADA, 2021) in Table 15 . DATS is also designed to work in conjunction with the Data Use Ontology. Bringing DATS and DUO together provides a formalisation of data access rules which are expected to work across CADRE settings, for multiple datasets in multiple disciplines. Gonzalez-Beltran et al. (2018) provide a sample mapping of content across health care, social science (including the Data Documentation Initiative standard used by ADA) and immunology.

Table 15 Applying the 3A's to the Australian Data Archive

Dimension	ADA Open	ADA General	ADA Special (e.g., Ten to Men)
Authorisation	None	Registration*	DUA signed by an individual
Authentication	None	Simple login	Simple login
Access	Download	Download	Download

**Authorisation may require additional specification. The current classification does not allow for specification of a data access request, but instead jumps from "registration" to "signed DUA"*

Secondly, the use of DATS and DUO in combination enables the specification of business rules for application by a data broker or custodian for processing of data access requests, along with a framework for the acceptance of terms of use through a data use agreement. The capacity to support an accepted agreement provides a key resource that is implicit in the Five Safes, but explicit in the proposed *Data Availability and Transparency Bill* – the exchange of a formalised agreement as a requirement of any data sharing.

The GA4GH group have leveraged this capability to allow for the exchange of such agreements. The GA4GH Passport specification (GA4GH, 2021a) has been developed to enable the exchange of researcher information, including "AcceptedTermsAndPolicies". The specification is a technical standard, using the metaphor of Passports and Visas as a means for understanding the information exchange. The specification provides:

> *a technical standard specifying a machine readable data format to attribute credentials to a person to validate their identity and verify that they are permitted to access data held by a third-party data custodian. The Passport specification further defines the mechanism by which such credentials are exchanged in a secure manner*

Notably, the GA4GH Passport includes a technical profile for authorisation and authentication (GA4GH, 2021b) including alignment with the OpenID Connect and OAuth 2.0 specifications.

Operationalising the Five Safes

In the Framework Structure section of this conceptual framework the core characteristics of each of the Five Safes are identified, along with two additional "Safes" for consideration, Organisations and Groups in the Extensions to the Five Safes section. In the "Joint and Several Application" of the Five Safes section, current information models are identified that address key characteristics associated with each Safe.

Operationalising the Five Safes framework involves the identification of relevant information standards, identifiers and schema and evaluating how existing and new information systems and services can be brought together to support researcher requests for access to sensitive data.

Table 16 and Table 17 present a summary of the permanent identifiers proposed for identification of each of the Five Safes, along with the key standards relevant to:

- Defining data custodian requirements for conditions of access, to define the information that should be provided for assessment (Table 16)
- Capturing or sourcing specific information on each Safe from a data user requesting access, define the means through which that information might be provided (Table 17)

The forthcoming CADRE information model will then fully specify the information requirements to be exchanged through the CADRE system.

Table 16 Potential information standards for defining data custodian requirements

Five Safes dimension	**Proposed identifier/PID**	**Custodian requirements specification**
People	ORCID	Data Use Ontology (DUO)
Projects	RAID, Funding ID, Local ID	Data Use Ontology (DUO), Data Tags Suite (DATS) CADRE configuration (RAID) & Setting configuration
Data	DOI, Handle	Setting configuration
Settings	RAID, Local ID	Data Tags Suite (DATS), Setting configuration
Outputs	DOI, Handle	Data Use Ontology (DUO)
Organisation	ROR	Data Use Ontology (DUO)
Group	Local ID	CADRE configuration

Table 17 Potential information standards and sources for sourcing information to meet requirements

Five Safes dimension	**Proposed identifier/PID**	**Information source for provision**
People	ORCID	AAF attributes, CADRE settings *Scholix/ResearchGraph (TBC)*
Projects	RAID	(CADRE specification) and CADRE Settings
Data	DOI, Handle	*DataCite, DCAT, Scholix/ResearchGraph, etc (TBC)*
Settings	RAID, Local	(CADRE specification), CADRE setting *Other existing standards (TBC)*
Outputs	DOI, Handle	*DataCite, DCAT, Scholix/ResearchGraph, etc (TBC)*
Organisation	ROR	*ROR specification (TBC)*
Group	Local	(CADRE specification), CILogon

(Sources in *italics* indicate potential sources for evaluation)

There are outstanding questions to be resolved regarding the choice of specific standards and where they fit into the data model. The expectation is that these questions will be resolved through CADRE Work Package 2, in the development of the information model.

Relevant standards, services and community driven informatics to consider include:

- REFEDS – Research and Education FEDerations (provided via AAF and used in authorisation and authentication systems in member organisations)
- Research Graph (schema developed by Research Graph)
- Data Use Ontology (DUO) and Data Tags Suite (DATS)
- RIF-CS – Registry Interchange Format – Collections and Services (used by ARDC for Research Data Australia service)
- SKOS – Simple Knowledge Organisation System (used by ARDC for Research Vocabularies Australia service)

- DDI – Data Documentation Initiative (used by ADA in the Dataverse system), DataCite (schema used by DataCite) and DCAT (schema used by data portal systems)
- CERIF – Common European Research Information Format (used by euroCRIS in Directory of Research Information Systems)
- Machine Actionable Data Management Plan application profile (including Access and Licence Indicators provided by NISO)

Questions for comment

There are a series of questions that will need to be resolved in the development of the information model and in particular how to encourage the creation and use of PID in research and research data management, and how to feed PID into and leverage the PID graph "a network of interconnected PID systems, as a basis for a wide range of services" (FREYA, n.d.).

1. *Regarding Researcher Identifier*

1.1. ORCID identifiers are largely applicable only to researchers in academia. Other sectors can use them – but potentially will not, as it is not relevant to their role, or to their access to the data.

1.2. There is a need to connect the data user's (researcher's) ORCID account to the institutional account and an endorsement.

2. *Regarding Activity Identifier*

2.1 Are RAID identifiers suitable for identifying Settings? (This question can be assessed in consultation with ARDC, whether a Safe Setting is a site that captures research activity related information).

2.2 How will the model connect the data user and use (project) to the institutional account and an endorsement?

2.3 Not all activities that involve the use of data are research projects e.g., student course work.

3. *Regarding Data Identifier*

3.1 Is there a need (and an interest) in specifying requirements for identifiers as part of data documentation standards – or is this a specific determination of the data custodian?

4. *Regarding Project Identifier*

4.1 What is the requisite identifier in this circumstance? In the absence of grant identifiers (e.g., Australian Research Council and National Health and Medical Research Council grants have persistent identifiers) which can be directly linked to a project, should project identifiers be created at the point a project is articulated to a Safe Setting where a sensitive data access request is made?

5. *Regarding Group Identifier*

5.1 There is no obvious model for either a permanent identifier or standards around groups. (CILogon, a candidate solution for managing groups, is a system, not a standard).

5.2 Groups are boundary objects, underpinned by organisational authorisation and instruments of control, but can be supra to an organisation, to enable inter-organisational collaboration and to cross jurisdictional lines. Group authority usually administered by an academic working as a Principal Investigator in an organisation where the responsibility for any legal and financial administration lies for research and by an academic delivering course work and supervising higher degree research students.

6. Regarding Organisation Identifier

6.1 There is expected to be within the DAT Act a requirement for accreditation of organisations. As noted earlier, the role of organisations as overseers, vetting site (driver's licence etc), instruments of control e.g., contract and policy. Organisations are where projects and groups are formulated, administered and authorised. How then are those organisational roles to be identified with the CADRE information model?

There is also a broader administrative question associated with the use of ORCID and RAID (persistent identifiers). There is currently only a limited (or even no) institutional process for endorsing information about the researcher (ORCID) or the project (RAID). As such, it is difficult for a data custodian (or broker such as ADA) to rely on this information as an authoritative source. While this capability develops within the sector, there may need to be mechanisms for capturing PID information. This may be one of the following forms:

- Collecting ORCID
- Connecting ORCID and RAID
- Using PID graph

ADA (for example) is currently capturing ORCID where they are provided voluntarily by data requestors and there are clear user and system wide benefits in capturing and linking DOI and ORCID to other research related PID e.g., RAID and local identifiers in systems within the national research infrastructure ecosystem.

Actioning Access

An explicit scope stipulation in this phase of the project is that the objective is ***not to automate access*** to data or research environments in the four systems being integrated with CADRE platform.

Rather, the CADRE information model is being developed to underpin decision-support. Where feasible to pass information between systems integrated with the CADRE platform to aid decision-support and improve user experience, this will be automated.

Options for extension to human initiated or automated functions are considered in the design but out of scope. Actioning access to data or research environments is deemed to be the responsibility carried by the setting owners and users of those systems.

Key Intersections

With key intersections between “Safes” a dominant feature of the information requirements, further investigation is needed to highlight how the combination of “Safe” information can best support an access request and/or oversight of a research environment and also highlight the need to draw in missing information.

Safe Person and Safe Data

This is a critical intersection of “Safe” information about people and data that aids decision-making and oversight, and this has implications for the interface design and data visualisation in the CADRE information exchange.

An assessment of a safe person is predicated on knowing:

- Relationships i.e., to an organisation, faculty and a supervisor.
- Readiness i.e., qualifications, skills, experience, training and accreditation.
- Roles and responsibilities i.e., student or researcher.
- Reliability i.e., a history of appropriate use of sensitive data and ethics approval.

An assessment of safe data is predicated on knowing:

- Project requirements and questions i.e., suitability of data.
- Research environment i.e., suitability of data treatment.
- Review of outputs i.e., suitability of data for release.

Key Alignments

Where there are key alignments between “Safes” and critical *additional* information is needed to make a determination, this is a different design challenge impacting the requestor and the data custodian or service provider. It will be important to address the difference between a person’s assertions and the ability to validate information from organisational and authoritative sources to establish trust, in the interface.

Information drawn from different sources will need to be clearly delineated in the interface to assist verification and a judgement on whether the source is trustworthy and/or when to seek more information to reduce risk or to act on the request.

Safe Person and Affiliation

- A person’s assertion of an affiliation to and a role in an organisation in an ORCID record versus the organisational assertion of that ORCID record supplied via an identity service provider used by the institution e.g., AAF or Microsoft.
- A person’s use of a non-institutional email versus the need to verify an institutional email address and match that against the request supplied via an identity service provider used by the institution e.g., AAF or Microsoft.

Safe Person and Training

- A person’s assertion of experience with sensitive data and/or a safe setting in a request application versus a record confirming their having successfully undertaken training from a recognised training, data or setting provider.
- A person’s assertion of group membership where sensitive data is used on a project versus confirmation from a senior researcher of membership and a role as a supervisor.

Safe Person and Ethics

- A person’s assertion a project has been put through an ethics assessment and evidence versus confirmation from the host organisation of an ethics approval.

Safe Person and Location

- A person’s assertion of research being undertaken in a location and evidence versus confirmation of the person’s location through IP tracing.

Data Access and Request Information

A data access request is a means for a requestor to provide information that can be validated and/or investigated further to assist with an access request. A data user can build up request information and a usage history record that can be reused and expedite future data access requests. There will be a need for a privacy impact assessment and some consideration on what user controls are in place for information to be retained and/or passed on between CADRE and the Safe Settings (in accord with service terms and conditions and privacy legislation).

Informatics

The metadata flowing into the CADRE information exchange is going to be a mixture of standardised attributes e.g., REFEDS provided by the research and education federations, community developed attributes e.g., Machine Actionable Data Management Plans developed through the Research Data Alliance, scholarly publisher attributes e.g., DataCite and funder attributes e.g., grant attributes provided by research councils. All of these systems support the capture of persistent (actionable and resolvable) identifiers (PID).

Information retained in local systems relating to e.g., terms and conditions of access, licences, projects, ethics assessments and training may be supplied in an access request but at this point it will not be possible to verify their status because of the absence of formal informatics and PID as attributes used in local systems. Useful information that lies in organisational registers need to be evaluated for use for verification e.g., Australian Business Register, Australian Charities and Not-For-Profits register, Tertiary Education Quality and Standards Agency register.

Any advances in formalising information retained within local systems and the use of authoritative registers and to include PID will assist with streamlining access request processes.

Analytics

The collation, analysis, and reporting of informatics to support the development of risk profiles for data custodians and data request types is in scope for the interface design of the CADRE information exchange. The aim is to enable risk assessments to be reviewed by each of the Safe Settings integrated with the CADRE platform and to lay a foundation for business rules to explored to streamline the data request and research environment oversight processes (Desai, Ritchie & Welpton, 2016 p.5).

> *The point is that the user has some idea of 'more safe data' and 'less safe data'. We return to the subjectivity of assessments in the penultimate section. There is an analogy in multi-criteria decision analysis (MCDA; see Ishazaka and Nemery, 2013, for a description, and Nutt et al (2015) for an example). MCDA recognises that the many factors affecting a decision might not be specified in ways which lead to simple numerical models of 'best' outcomes. As such decision-making is explicitly subjective, expert-based, and negotiated across incompatible dimensions. An alternative analogy was provided by McEachern (2015), who proposed that the model is akin to a graphic equaliser*

Limitations and Additional Requirements

- As the project moves into operationalisation scalability issues may arise with risk averse case-by-case approaches to access request management and limitations on capacity to share information across systems.
- Changes to the metadata available from different information sources over time may impact the analytics and data visualisation (interface design), and ongoing user feedback will be critical.
- Moving from principle to practice is likely to expose unseen assumptions implicit in the information model and in combination with changes to metadata supplied, it is likely a regular review of the information model will be needed.

Appendices

Partner Information

The CADRE framework (and the information architecture) is shaped by the concepts embedded in the Five Safes principles and informed by CADRE partners information requirements.

- What information do sensitive **data custodians or brokers** need (from researchers) to determine how and/or whether to make sensitive data accessible to them and how do they monitor usage and outputs?

- What information do **research environment managers** need to provide to support researchers seeking to provide evidence of due diligence (to data custodians or brokers)?

- What information do **researchers** need to have collated and linked together so that they can produce historical records of their data usage, their affiliation, training, ethics approval, research experience, and scholarship (for data custodians or owners)?

Each CADRE partner brings a unique set of interests, responsibilities, and requirements and these are captured as use cases. The use cases serve as inputs to the framework design and information architecture development processes.

Each use case aids in the development of a grounded and multi-perspectival view on the Five Safes conceptually and in identifying important information components in common. For example, to understand if a person is safe: key information about the requestor is needed like their personal name, education level, and organisational affiliation – and – the source of that information. This type of information is a common requirement in all of the use cases.

All the CADRE partners need to have information about the researcher (as sensitive data requestor) – this is a first order question. The second order question directly following is – what does the data requestor seek to do with sensitive data? The third order question (based on answers to questions one and two) is – what authorisation is therefore appropriate and how can access be best controlled and enabled?

Partner Use Cases

Use cases from each CADRE partner help to ascertain commonality and variation around using the Five Safes framework for decision-making. Some CADRE partners will have more than one use case to aid the decision-support development in the CADRE information exchange within the platform and those outlined in the CADRE framework are indicative only (and not exhaustive).

Studies of Childhood, Education and Youth (SOCEY) – Accessing Qualitative Sensitive Data

Access to personal data

Education/history/sociology research drawing upon oral interviews and associated data, which can include material culture (including drawings, photographs, and other objects created by a participant), generates largely qualitative (and some mixed methods) data. The *National Statement on Ethical Conduct in Human Research* (2007) (hereafter *National Statement*) defines qualitative research as that "involving the ... use of empirical materials such as case studies, personal experience, life stories, interviews, observations, and cultural texts (NHMRC, 2018b, p.103). Research projects in the field of childhood, education and youth (and others) might comprise audio and video recordings, transcripts, images, biographical information, maps, timelines and more.

The data generated through interview is rich with personal expression and meaning, and references social insight, experience, phenomena, and people. Due to the richness of this data, the risk associated with it is high but also has great potential for sharing and re-use either current moment or historically.

The nature of qualitative data means that it can be highly sensitive as there are numerous direct and indirect means of identifying a participant and third parties mentioned or implicated. Even when anonymised, this data might still render a participant or third party as identifiable. As Kirilova and Karcher (2017) observed when discussing the Five Safes in relation to the Qualitative Data Repository (QDR) managed by Syracuse University, it is difficult to render qualitative data and its outputs completely safe. The QDR Curation Policy outlines that storage and re-use of qualitative data requires a range of strategies for rendering it *safer*: informed consent; de-identification (if required); and access controls (QDR, n.d., para 6–8).

The *National Statement* (NHMRC, 2018b, s3.1.37) acknowledges the potential value of retaining and re-using data and indicates:

> *When researchers seek consent to collect information that is considered to be of historical, cultural or other long-term value, they should obtain consent for its perpetual retention, including any planned re-use and sharing with others.*

In the qualitative data realm, the removal of identifiers often concomitantly reduces or negates the value of the data, for which the context is vital to understanding, and would be considered essential for long-term value. In the discussion paper, *Doing Research Differently*, the authors explore the value of qualitative data for both immediate projects and future research. Permanent de-identification is not always ideal and, in fact, may be detrimental to the data value (McLeod et al., 2020, p.15; see also Corti et al. 2000). They recommend that the key to preserving and rendering the data useful is to apply various strategies similar to but building on those suggested by the QDR and the *National Statement* (McLeod et al., 2020, p.24–25).

While it may be difficult to render qualitative data or its outputs completely safe, it is vital when dealing with such data to (Kirilova and Karcher, 2017):

> *educat[e] researchers how to be "safe people" and how to plan for "safe projects" – when accessing such data and using them for secondary analysis – and providing long-term "safe settings" for the data, including via de-identification and appropriate access controls*

Of significant importance is seeking detailed informed consent from participants for identification, recording of interviews, ongoing data retention, future access for research, and use in outputs. Permission identification, ongoing data retention and re-use could be denied outright by participants and/or conditions agreed for future access. Multiple levels of detailed consent are often required to cover sharing, use, re-use now and in the future. These work together with access levels in a repository to render the data and project safer.

Interview data retained for future access can be subject to access conditions that link safe concepts together such that a research project can be viewed as safe. A Safe Project serves as an umbrella concept for safety considerations and assessing whether access is permitted.

Access Condition	Safe Data	Safe People	Safe Project	Safe Output	Safe Setting
Data remains "as is" and any research usage permitted under a confidentiality agreement.	🟩	🟩	🟩		
Identifying data of all persons is redacted to address privacy concerns and any research usage by permission.			🟩	🟩	
Data remains "as is" and only research allied original data collection is permitted.	🟩	🟩	🟩		
Data remains "as is" and may only be viewed through institutional systems remotely.	🟩		🟩		🟩
Identifying data of all persons and places is anonymised, data is published and usable for research by permission.			🟩	🟩	

Two examples of strategies to preserve the richness of the data for future research are: to seek permission from participants to be readily identified with their data or to de-identify data for any use up to a certain period of time, after which the full data might be released. These are strategies adopted by a number of projects deposited in the SOCEY Repository hosted by the Australian Data Archive (SOCEY, n.d.). In one case, most participants agreed to be fully identified in the research and outputs, while in another, participants agreed to their de-identified data being made available after fifty years (McLeod et al. 2020, p.15–19).

Interview data retained for future access may be subject to a range of conditions (based on consent given) and several pieces of information embedded in an access request need to be viewed together such that a research project is viewed as safe, and data can be made available (or if the data is modified as a pre-emptive risk mitigation).

Information embedded in a data access request:

- Researcher information
- Project information
- Ethics application
- Data management plan
- Training and experience

Access Condition	Researcher information	Project description	Ethics application	Data management plan	Training and experience
Data remains "as is" and any research usage permitted under a confidentiality agreement.	🟩	🟩	🟩	🟩	🟩
Identifying data of all persons is redacted to address privacy concerns and any research usage by permission.	🟩	🟩			
Data remains "as is" and only research allied to the original data collection is permitted.	🟩	🟩	🟩	🟩	🟩
Data remains "as is" and may only be viewed through institutional systems remotely for related research.	🟩	🟩	🟩	🟩	🟩
Identifying data of all persons and places is anonymised, data is published and usable for research by permission.	🟩	🟩			

Australian Data Archive (ADA) – Public Benefit/Interest Test

The Australian Data Archive receives requests for access to data and a "public benefit/interest" test is applied when making sensitive data accessible for research undertaken by government, higher education institutions, non-governmental agencies or private organisations. The ADA seeks information to assist with the decision-making process including information pertaining to the person/requestor including but not limited to identities, organisational affiliation e.g., University ID, Google ID or ORCID. The request process involves researchers responding to questions in a webform in the dissemination system (Dataverse) and through follow up email exchanges. A Request Access app (proof of concept) with a new webform is in development to support automatic and/or easy capture of request information that has previously been completed in this system or that is available for linking from another system (such as AAF) in an attempt to reduce the form filling load on researchers and to streamline the request process. This will allow information to be automated and transferred between relevant systems that utilise the same information. There are different data points and information to collect that can be understood as three of the Five Safes: Safe People, Safe Projects, and Safe Settings, for example:

Data Points and Information	Safe Data	Safe People	Safe Project	Safe Output	Safe Setting
Identities of the requestor and data users		🟩			
Affiliation of requestor with other data requestors		🟩			
Affiliation with an organisation (academic, NGO, commercial, etc) or a research project		🟩	🟩		
Intended use of the data that drives the access request			🟩		
Provision of secure location for data storage and processing for the duration of the project					🟩

ADA user services review, validate, and verify data points associated with these three "Safes" to inform and base a data access request decision (authorisation to use). At the same time, they review:

Data Points and Information	Safe Data	Safe People	Safe Project	Safe Output	Safe Setting
The data owner/depositor warrants consent process has ensued in the deposit process (as access conditions are set).	🟩				
The need for curatorial intervention to mitigate risk of breach in consent or personal disclosure.				🟩	
Business rules developed with the data owner to facilitate access.					🟩

Information for decision support is in numerous systems i.e., within ADA (Dataverse, the internal wiki) and external to ADA, in research management systems (ethics applications), scholarly publication databases, and the world wide web. ADA user services treat access requests on a case-by-case basis currently and work manually. In the development of a request access management app and integration with the CADRE platform ADA aims to move towards systematic recordkeeping and to enable requestors to draw their own historic request and usage information into new requests automatically.

Australian Institute of Family Studies (AIFS) – Data Releases & Linkage

Sensitive data arising from the *Ten to Men* study (*The Australian Longitudinal Study on Male Health*) is commissioned by the Department of Health, then curated and managed by AIFS, and disseminated by ADA to ~200 researchers. Data access requests go to an AIFS committee that work through broad questions to assess safety and the decision is passed onto ADA to action in a “Facilitated” arrangement. AIFS determines which requestors will be permitted access to the data and ADA facilities the access via the Dataverse system. ADA requires all persons on the list received from AIFS to set up and verify a Dataverse account from which data access will be given. When new data from the *Ten to Men* study is made accessible for research (by AIFS) access conditions around prior files (data) is closed off (by ADA). Existing data users are informed of the changes and the data release information is captured in metadata and documentation (by ADA) and on occasion where errors have been detected and so the data is not disclosive, there are new versions of the release supplied. The relationship between three of the Five Safes: Safe Data, Safe Projects, and Safe Outputs is revisited each time there is an update or a change to the dataset where there has been or is in use. This limits the likelihood reproducibility and disclosure issues arising. Updating “active” (in progress) requests is under consideration (by ADA) for the data request and dissemination processes.

Sensitive Data – Updates and Changes	Safe Data	Safe People	Safe Project	Safe Output	Safe Setting
New data release	🟩		🟩	🟩	
New data release version	🟩		🟩	🟩	
Data linkage	🟩		🟩	🟩	
Project updates (relating to people, data linkages, setting or research focus)	🟩		🟩	🟩	

Sensitive data arising from the *LSAC* study (*Longitudinal Study of Australian Children aka Growing Up in Australia*) is commissioned by the Department of Social Services (National Centre for Longitudinal Data), then curated and managed by AIFS, and disseminated by ADA to ~2500 researchers. *LSAC* is a large-scale dataset, there are multiple parties involved in the supply chain, and AIFS is a Commonwealth integrating data entity (data linkage). Requests via ADA (to AIFS) for data linkage (with *LSAC*) can include to linking survey, geo-spatial or administrative data, and may involve securing participant consents. Linked data is a one-off exercise, and it is not on-shared (by AIFS) and deposited with ADA for wider dissemination.

AARNet Sensitive Data Service (SDS) – Streamlining Research Workflows

AARNet is developing a sensitive data service to meet growing researcher demand for a secure service to store, analyse and share sensitive data. Familiar categories of sensitive data are data concerning human participants, data relating to species of plants or animals, culturally sensitive data and commercially sensitive data. A secure research environment requires social and technical safety requirements that deal with issues relating to authorisation management, risk mitigation, auditability, and cybersecurity.

Researchers' need to comply with data providers' access conditions (already established through a data access request system and process) and "translate" those access conditions into authorisation arrangements within a secure research environment. These access conditions must be reflected in the level of authorisation (access and use) that is enabled within the secure setting.

All parties involved in managing and maintaining a sensitive data setting have responsibility to support access, compliance, and limit data breach (OAIC, n.d.). Streamlining the process of project setup, review, and closure is desirable for secure setting providers (platform owner), administrators (the tenants) and users (the researchers).

The current system roles in the SDS Proof of Concept (POC) reflect the interleaved layers of technical and authorisation management.

- Global admin (AARNet support)
- Tenant admin (Institution)
- Principal authoriser
- Collaborator
- Viewer

The researcher user experience and research workflow can be improved through the CADRE platform by increasing information flow across and between systems for verification and validation. Example information includes request and authorisation information e.g., parties and roles, affiliations, project description, access level settings, duration setting, audit and output requirements

Systems	Secure Setting – Data Archive	Five Safes Setting	Secure Setting – Research Environment
High level process	Provisioning	Decision-support	Provisioning
Scenario	Australian Data Archive	CADRE	Sensitive Data Service
Sub processes	• Data request • Data release (via transfer) • Authorisation enabled (via access conditions) • Monitoring (via shared custody)	• Request information • Authorisation information • Risk management heuristics	• Environment request • Data receipt and output deposit (via transfer) • Authorisation arranged (via access conditions) • Compliance (via shared custody)

Other use cases for future development include cases from AIHW, CBDRH, AURIN and Data CO-OP.

Australian Institute of Health and Welfare (AIHW)
[Use case: applications for data linkage TBC]

UNSW Centre for Big Data Research in Health (CBDRH)
[Use case: SRAE & ERICA and accreditation and safe settings usage information TBC]

Australian Urban Research Infrastructure Network (AURIN)
[Use case: group access to data and research environment TBC]

Swinburne University (Data CO-OP)

[Use case: research use of data insights TBC]

Sensitive Data Categories

Data owners, custodians and brokers have varying categorical descriptions that express the different sensitivity ratings of data in their control. In various pieces of Australian legislation terminology is defined to capture the nature of the personal data, privacy impacts and government record keeping and security classifications. In this section category terminology is collated from each Safe Setting that will be integrated with the CADRE Platform to assist with shared understanding of the spectrum of sensitivity and curatorial safety concerns (and the respective controls applied in authorisation, authentication and access processes).

Australian Data Archive (ADA)

General Release

Studies with controlled data access managed by the ADA on behalf of the depositor.

This version of the data must be fully de-identified, have minimal or no disclosure risk, have no direct identifier and no indirect identifier at an agreeable level (cell size 3 as standard)

De-Identification: A process involving the removal of Direct Identifiers from the data followed by one or both of the following steps:

- The removal or alteration of other information that could potentially be used to re-identify an individual, and/or
- The use of controls and safeguards in the data access environment to prevent re-identification.

Resulting in no reasonable likelihood of re-identification.

Disclosure Risk: The combination of likelihood and consequence that information about an individual, organisation or other entity is revealed or provided to an unauthorised person, organisation or entity. Typically occurs in two common forms, re-identification or attribute disclosure.

Direct Identifier: Information which, by itself, is able to uniquely identify an individual, organisation or other entity. Examples of direct identifiers include but are not limited to name, address, latitude/longitude, driver’s license number and Australian Business Number (ABN).

Indirect Identifier: Information that can be used to identify an individual, organisation or other entity with a high probability, either alone or together with other indirect identifiers, and in combination with auxiliary information.

Particularly Sensitive Data: Any data where unauthorised disclosure would likely lead to adverse consequences for the individual, organisation or Australia in general. Data which is of a personal, legal, commercial, security or environmental nature may be considered particularly sensitive. This is broader than the Privacy Act 1988 definition of sensitive data which is defined as a subset of personal information and limits how it can be collected and used.

Personal Information: Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) Whether the information or opinion is true or not true; and

(b) Whether the information or opinion is recorded in a material form or not.

This might include information such as a person’s name and address, medical records, bank account details, photograph, videos, where they work and even what they like. Under the Privacy Act 1988, this term can only refer to living individuals. For the ADA, the assumption is that all persons are still living, unless the information is of such an age that this is impossible. For example, the information is from a poll conducted in 1819, making the participant 200 years old in 2019.

Reasonably Identifiable: An individual will be considered to be reasonably identifiable within a dataset for the purposes of the definition of Personal Information where:

(a) It is technically possible for re-identification to occur (whether from the information in the dataset itself, or in combination with other information that may be available); and
(b) There is a reasonable likelihood that this might occur.

Re-Identification: The discovery of the identity of an individual, organisation or entity in an apparently de-identified dataset, whether through a targeted attack or unintentionally, using publicly or privately held information about that individual, organisation or entity.

Response Knowledge: The knowledge that a population unit is included within a dataset. This could be through private knowledge (e.g., a friend or work colleague has mentioned that they responded to a particular survey), or it could be through simple knowledge that a particular population unit is a member of the population and the data is a full dataset for that population (e.g., a census). For the purposes of clarity, a population unit is any one member (unit) of a set of items (population) that is being studied. This can relate to a person, entity or organisation.

Sensitive Information: A specific sub-set of Personal Information under the Privacy Act 1988 that includes:

(a) Information or an opinion about an individual’s
    i. Racial or ethnic origin; or
    ii. Political opinions; or
    iii. Membership of a political association; or
    iv. Religious beliefs or affiliations; or
    v. Philosophical beliefs; or
    vi. Membership of a professional or trade association; or
    vii. Membership of a trade union; or
    viii. Sexual orientation or practices; or
    ix. Criminal record;
(b) Health information about an individual; or
(c) Genetic information about an individual that is not otherwise health information; or
(d) Biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
(e) Biometric templates.

Restricted Release

Studies where the depositor, or an authorised representative, wishes to be informed by the Archive of each request to use the data in order to give or withhold permission.

Special

Studies where the depositor has included additional special access conditions. For example, the user may be required to obtain the permission in writing of the original depositor of the data, or an authorised representative, before publishing any interpretation of such materials.

Australian Institute of Health and Welfare (AIHW)

[Examples of broad sensitive data categorisation TBC]

Australian Institute of Family Studies (AIFS)

[Examples of broad sensitive data categorisation TBC]

Australian Urban Research Infrastructure Network (AURIN)

[Examples of broad sensitive data categorisation TBC]

UNSW Centre for Big Data Research in Health (CBDRH)

[Examples of broad sensitive data categorisation TBC]

Terminology

Access agreements – agreements made between a data owner or broker and the data user that enable access to data e.g., terms of use, account privileges, licencing

Access conditions – guidelines and rules set in place by the data owner or broker to determine whether an access request can be made

Anonymisation – changes to data with the intent on protecting privacy that may include removal of information that directly or indirectly makes a person identifiable

Authorisation and authentication – the processes by which access to a resource is enabled through permission identity and checks i.e., validation and verification. Also referred to as AuthN/AuthZ.

Commercial benefit or interest – the intent driving a request for access to data for research is for private gain

Commercial risk – relating to business, reputational, financial, or legal damage to a person or an organisation that arises through making data accessible or misusing data

Confidentiality risk – data is provided in confidence and a person may directly or indirectly be identifiable, the risk of being identified is assessed to maintain the trust of data providers (and confidentiality)

Curatorial treatment – data is worked on and altered to enable preservation, improve its reusability, obscure personally identifying information, etc

Data disclosure – data is made available that includes private or personally identifying information that was provided under confidentiality

Data sharing program – data sharing is formalised into a program with documented procedures, governance policies and an authorisation process

Deidentified data – TBC

Disclosure risk – TBC

Ethics application – TBC

Institutional affiliation – TBC

Metadata – TBC

Paradata – TBC

Privacy impact assessment – TBC

Privacy preserving security – TBC

Public benefit or interest – TBC

Remote access facility – TBC

Remote processing – TBC

Reputational risk – TBC

Research program – TBC

Research project – TBC

Researcher passport – TBC

Safety after – TBC

Safety before – TBC

Safety during – TBC

Secure data products – TBC

Secure enclave – TBC

Sensitive data products – TBC

Statistical disclosure control – TBC

Track record – TBC

References

Alter, G., Gonzalez-Beltran, A., Ohno-Machado, L. & Rocca-Serra, P. (2020). The Data Tags Suite (DATS) model for discovering data access and use requirements, *GigaScience*, 9 (2),1-10. DOI: 10.1093/gigascience/giz165

Australian Bureau of Statistics (2011). *Census of the Commonwealth of Australia*, 1911. https://www.abs.gov.au/AUSSTATS/abs@.nsf/mf/2112.0

Australian Bureau of Statistics (2013). *Methodology for the Automatic Confidentialisation of Statistical Outputs from Remote Servers at the Australian Bureau of Statistics*. Joint UNECE/Eurostat work session on statistical data confidentiality [Working Paper] (Ottawa, Canada, 28-30 October 2013). Prepared by Gwenda Thompson, Stephen Broadfoot and Daniel Elazar, Australian Bureau of Statistics, Australia. https://www.unece.org/fileadmin/DAM/stats/documents/ece/ces/ge.46/2013/Topic_1_ABS.pdf

Australian Bureau of Statistics (2017). *ABS Confidentiality Series*, Aug 2017. https://www.abs.gov.au/ausstats/abs@.nsf/mf/1160.0

Australian Bureau of Statistics (2021). *Microdata and TableBuilder* https://www.abs.gov.au/statistics/microdata-tablebuilder

Australian Bureau of Statistics (2021). *DataLab safe researcher training*, 21 October 2021. https://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/1406.0.55.007Main%20Features10User%20Guide?opendocument&tabname=Summary&prodno=1406.0.55.007&issue=User%20Guide&num=&view=

Australian Institute of Aboriginal and Torres Strait Islander Studies (2020). *Code of Ethics for Aboriginal and Torres Strait Islander Research*. https://aiatsis.gov.au/research/ethical-research

Australian Institute of Family Studies & Department of Health (2021). Ten to Men, The Australian Longitudinal Study on Male Health. https://tentomen.org.au/

Australian Institute of Health and Welfare (2021). *The Five Safes framework*. https://www.aihw.gov.au/about-our-data/data-governance/the-five-safes-framework

Biddle, N., Edwards, B., Gray, M. C. & McEachern, S. (2018) Public attitudes towards data governance in Australia, *CSRM Working Paper* no. 12/2018. http://csrm.cass.anu.edu.au/sites/default/files/docs/2018/12/CSRM-WP-DATAGOVERNANCE-PUBLISH_0.pdf

BioCADDIE (Biomedical and Healthcare Data Discovery Index Ecosystem) (n.d.) https://dbmi.ucsd.edu/projects/biocaddie.html

Bond, S., Brandt, M., & de Wolf, P. (2013) *Guidelines for the checking of output based on microdata research.* Data Without Boundaries, FP7/2007-2013, WP11.8, Guidelines for Output Checking (Improved Methodologies for Managing Risks of Access to Detailed OS Data) https://ec.europa.eu/eurostat/cros/system/files/dwb_standalone-document_output-checking-guidelines.pdf

Butler-Henderson, K. & Gray, K. (2018). *Australia's Health Information Workforce: Census Summary Report*, 2018. https://www.hisa.org.au/wp-content/uploads/2018/11/Australias-HIW-Census-Summary-Report-2018.pdf

Churches, T. & Jorm, L. (2019) Locking the front door without leaving the windows open: positioning authentication technologies within the "Five Safes" framework for effective use of sensitive research data, 20 November 2019. DOI: 10.5281/zenodo.3547979

CILogon (n.d.) CILogon: An Integrated Identity and Access Management Platform for Science, https://www.cilogon.org/

Corti, L., Day, A. & Backhouse, G. (2000) Confidentiality and Informed Consent: Issues for Consideration in the Preservation of and Provision of Access to Qualitative Data Archives. FORUM: Qualitative Social Research Sozialforschung 1.3. **DOI:** https://doi.org/10.17169/fqs-1.3.1024

Council of Australasian University Information Technology Directors (CAUDIT) (2019). Identity Access Management Community, https://www.caudit.edu.au/news/identity-access-management-community

Courtet, M. (2021) Powering up data discovery and access using the Data Use Ontology. https://www.cineca-project.eu/blog-all/powering-up-data-discovery-and-access-using-the-data-use-ontology

Culnane, C., Rubinstein, B. I. P, & Teague, V. (2017). Health data in an open world, 15 December 2017. https://arxiv.org/abs/1712.05627

Culnane, C., Rubinstein, B. I. P, & Teague, V. (2020). Not fit for purpose: a critical analysis of the 'Five Safes', 4 November 2020. https://arxiv.org/abs/2011.02142

Curtin University (n.d.) SeRP@Curtin. https://healthsciences.curtin.edu.au/health-sciences-research/research-institutes-centres/data-analytics-hub/serp-curtin/

Dabla-Norris, E, Federico J. D., & Duval, R. 2020. "The use of administrative data at the International Monetary Fund" In: Cole, Dhaliwal, Sautmann, and Vilhuber (eds), *Handbook on Using Administrative Data for Research and Evidence-based Policy*. https://admindatahandbook.mit.edu/book/latest/imf.html

DUO (Data Use Ontology) (2021a) https://github.com/EBISPOT/DUO

DUO (Data Use Ontology) (2021b) http://purl.obolibrary.org/obo/duo.owl

DUO (Data Use Ontology) (2021c) Health or medical or biomedical research http://purl.obolibrary.org/obo/DUO_0000006

Department of Health (n.d.) *Australian Longitudinal Study on Male Health.* https://www.health.gov.au/health-topics/preventive-health/population-health-studies#australian-longitudinal-study-on-male-health-

Department of Health (n.d.) *ERICA Training*, https://www.openlearning.com/unswmed/courses/erica-training/?cl=1

Department of Prime Minister and Cabinet (PM&C) (2018). *The Australian Government's Response to the Productivity Commission Data Availability and Use Inquiry*. https://dataavailability.pmc.gov.au/sites/default/files/govt-response-pc-dau-inquiry.pdf

Department of Social Services (n.d.) *Growing Up in Australia: The Longitudinal Study of Australian Children (LSAC)*. https://www.dss.gov.au/about-the-department/publications-articles/research-publications/longitudinal-data-initiatives/footprints-in-time-the-longitudinal-study-of-indigenous-children-lsic/growing-up-in-australia-the-longitudinal-study-of-australian-children-lsac

Desai, T., Ritchie, F., & Welpton, R. (2016). Five Safes: designing data access for research, 29 January 2016. http://www1.uwe.ac.uk/bl/research/bristoleconomicanalysis/economicsworkingpapers/economicspapers2016.aspx

FREYA (n.d.) *The PID Graph*, https://www.project-freya.eu/en/pid-graph/the-pid-graph

Garfinkel, S., Abowd, J. M., & Martindale, C. (2019). Understanding database reconstruction attacks on public Data. *Communications of the ACM*, March 2019, 62(3), 46-53. DOI: 10.1145/3287287

Generation Victoria (2019). The benefits of GenV's Data Repository. https://genv.org.au/for-researchers/the-benefits-of-the-genv-data-repository/

Global Alliance for Genomics and Health (GA4GH) (2021a). GA4GH Passport, v1.0.2. https://github.com/ga4gh-duri/ga4gh-duri.github.io/blob/master/researcher_ids/ga4gh_passport_v1.md

Global Alliance for Genomics and Health (GA4GH) (2021b). GA4GH OpenID Connect Protocol, v1.0.4. https://github.com/ga4gh/data-security/blob/master/AAI/AAIConnectProfile.md

Global Alliance for Genomics and Health (GA4GH) (2021c). Researcher Identities: GA4GH Passports and Visas. https://github.com/ga4gh-duri/ga4gh-duri.github.io/tree/master/researcher_ids

Goldmann, G. (2009/10) From a seed to a forest: Microdata access at Statistics Canada. *Statistical Journal of the IAOS*, 26(3/4), 75-87. DOI: 10.3233/SJI-2009-0703.

Gonzalez-Beltran, A. N., Campbell, J., Dunn, P., Guijarro, D., Ionescu, S., Kim, H., Lyle, J., Wiser, J., Sansone, S., & Rocca-Serra, P. (2018) Data discovery with DATS: exemplar adoptions and lessons learned. *Journal of the American Medical Informatics Association*, 25(1), 2018, 13–16. DOI: 10.1093/jamia/ocx119

Government of South Australia (GSA), Department of the Premier and Cabinet (n.d.). Sharing public sector data, https://www.dpc.sa.gov.au/responsibilities/data-sharing/information-sharing-in-south-australia/sharing-public-sector-data

Government of Victoria (GV) (n.d.). Navigating legislation and sharing safely, https://www.vic.gov.au/navigating-legislation-sharing-safely

Green, A. G. & Gutmann, M. P. (2007). Building partnerships among social science researchers, institution-based repositories and domain specific data archives, *OCLC Systems & Services*, 23(1),35-53. DOI: 10.1108/10650750710720757

Griffiths, E., Greci, C., Kotrosios, Y., Parker, S., Scott, J., Welpton, R., Wolters, A. & Woods, C. (2019) *Handbook on Statistical Disclosure Control for Outputs*. UK Data Archive, v1.0, July 2019. https://ukdataservice.ac.uk//app/uploads/thf_datareport_aw_web.pdf

Hasani-Mavriqi, I., Sokolovska, N., Ross-Hellauer, R. & Fecher, B. (2020) Challenges in building innovative sustainable and open research infrastructures. *Elephant in the Lab*, 18 February 2020. DOI: 10.5281/zenodo.3685642

Indigenous Data Network (n.d.) https://mspgh.unimelb.edu.au/centres-institutes/centre-for-health-equity/research-group/indigenous-data-network

International Standards Organisation (ISO) (n.d.) ISO/IEC 27001, Information Security Management, https://www.iso.org/isoiec-27001-information-security.html

Kirolova, D & Karcher, S. (2017) Rethinking Data Sharing and Human Participant Protection in Social Science Research: Applications from the Qualitative Realm, *Data Science Journal* 16, 43. DOI: 10.5334/dsj-2017-043

Levenstein, M. C., Tyler, A. R. B., & Bleckman, D. J. (2018) *The Researcher Passport: Improving Data Access and Confidentiality Protection: ICPSR's Strategy for a Community-normed System of Digital Identities of Access.* ICPSR White Paper Series No. 1. https://hdl.handle.net/2027.42/143808

McLeod, J., O'Connor, K., & Davis, N. (2020) *Doing Research Differently: Archiving & Sharing Qualitative Data in Studies of Childhood, Education and Youth*. University of Melbourne. DOI: 10.25916/5e9e28eec21a1

McEachern, S. (2018) Enabling access to sensitive data at the Australian Data Archive, *eResearch Australasia 2018 Conference*, https://conference.eresearch.edu.au/wp-content/uploads/2018/10/ADA_SensitiveData_eResearch2018_edited.pdf

Müller, D., & vom Berge, P. (2020). "Institute for Employment Research, Germany: access to administrative labor market data for international researchers." In: Cole, Dhaliwal, Sautmann, and Vilhuber (eds), *Handbook on Using Administrative Data for Research and Evidence-based Policy*. https://admindatahandbook.mit.edu/book/v1.0-rc6/iab.html

National Health & Medical Research Council (2018a). *Australian Code for the Responsible Conduct of Research*, https://www.nhmrc.gov.au/about-us/publications/australian-code-responsible-conduct-research-2018

National Health & Medical Research Council (2018b). *National Statement on Ethical Conduct in Human Research (2007)*, https://www.nhmrc.gov.au/about-us/publications/national-statement-ethical-conduct-human-research-2007-updated-2018

National Health & Medical Research Council (2019) *Management of Data and Information in Research: a Guide supporting the Australian Code for the Responsible Conduct of Research*, https://www.nhmrc.gov.au/sites/default/files/documents/attachments/Management-of-Data-and-Information-in-Research.pdf

New South Wales Government (2015). *Data Sharing (Government Sector) Act 2015*. https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2015-060

New South Wales Government (2021). Data.NSW https://data.nsw.gov.au/

National Opinion Research Centre (NORC) (n.d.). *Secure and Remote Data Access and Disclosure Avoidance*, University of Chicago https://www.norc.org/Research/Capabilities/Pages/strategic-communications-and-dissemination/secure-and-remote-data-access-and-disclosure-avoidance.aspx

National Opinion Research Centre (NORC) (n.d.). *Secure Data Dissemination and Access*, University of Chicago https://www.norc.org/Research/Capabilities/Pages/strategic-communications-and-dissemination/secure-data-dissemination-and-access.aspx

Office for National Statistics (ONS) (2017). The 'Five Safes' – data privacy at ONS, 27 January 2017. https://blog.ons.gov.uk/2017/01/27/the-five-safes-data-privacy-at-ons/

Office of the Australian Information Commissioner (OAIC) (n.d.). Data breaches. https://www.oaic.gov.au/privacy/data-breaches/

Office of the National Data Commissioner (ONDC) (2019). *Best Practice Guide to Applying Data Sharing Principles*, 15 March 2019. https://www.datacommissioner.gov.au/sites/default/files/2019-08/data-sharing-principles-best-practice-guide-15-mar-2019.pdf

Office of the National Data Commissioner (ONDC) (n.d.). *Data Availability and Transparency Bill*, https://www.datacommissioner.gov.au/data-legislation/data-availability-and-transparency-bill

Office of the National Data Commissioner (ONDC), (2020a). *Accreditation Framework Discussion Paper*. Commonwealth of Australia, September 2020. https://www.datacommissioner.gov.au/sites/default/files/2020-09/Accreditation%20Framework%20Discussion%20Paper.pdf

Office of the National Data Commissioner (ONDC), (2020b). *Data Availability and Transparency Bill 2020 Exposure Draft, Consultation Paper*, September 2020. https://www.datacommissioner.gov.au/sites/default/files/2020-09/DAT%20Bill%202020%20exposure%20draft%20Consultation%20Paper%20Final_0.pdf

O'Hara, A. (2019). *Postsecondary Data Infrastructure: What is Possible Today*. The Institute for Higher Education Policy. http://hdl.handle.net/10919/95136

O'Keefe, C. M., Otorepec, S., Elliot, M., Mackey, E. & O'Hara, K. (2017) *The De-Identification Decision-Making Framework*. CSIRO Reports EP173122 and EP175702. https://www.data61.csiro.au/en/Our-Work/Safety-and-Security/Privacy-Preservation/De-identification-Decision-Making-Framework

Parker, T. (2017). The DataLab of the Australian Bureau of Statistics. *Australian Economic Review*, 50(4), 478-483. DOI: 10.1111/1467-8462.12246

Parliament of Australia (PA) (2020), *Data Availability and Transparency Bill 2020*, https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6649

Qualitative Data Repository (QDR) (n.d.). *Human Participants: General Guidance*, https://qdr.syr.edu/guidance/human-participants

Research and Education FEDerations (REFEDS) (2021) Welcome to the REFEDS Wiki, https://github.com/RDA-DMP-Common/RDA-DMP-Common-Standard

Research Data Alliance (2021) RDA DMP Common Standard for Machine-Actionable Data Management Plans, https://github.com/RDA-DMP-Common/RDA-DMP-Common-Standard

Ritchie, F. & Elliot, M. (2015). *Principles- versus rules-based output statistical disclosure control in remote access environments.* Working Papers 20151501, Department of Accounting, Economics and Finance, Bristol Business School, University of the West of England, Bristol. https://ideas.repec.org/p/uwe/wpaper/20151501.html

Ritchie, F. (2017) The 'Five Safes': a framework for planning, designing and evaluating data access solutions, *Data for Policy 2017 Conference* DOI: 10.5281/zenodo.897821

Ritchie, F. & Green, E. (2016). *Department of social services data access project final report*, Project Report, 6 September 2016. https://uwe-repository.worktribe.com/output/908255

Ritchie, F. & Green, E. (2020). *Frameworks, principles and accreditation in modern data management*, https://www2.uwe.ac.uk/faculties/BBS/BUS/Research/BCEF/Frameworks.pdf

Ritchie, F., Green, E., Newman, J., & Parker, T. (2017) *Lessons learned in training 'safe users' of confidential data*. https://unece.org/fileadmin/DAM/stats/documents/ece/ces/ge.46/2017/7_lessons_learned_training.pdf

Ritchie, F. & Tava, F. (2020) Five Safes or One Plus Four Safes? Musing on project purpose, 27 July 2020, Bristol Centre for Economics and Finance blog. https://blogs.uwe.ac.uk/economics-finance/five-safes-or-one-plus-four-safes-musing-on-project-purpose/

Ruggles, S., Fitch, C., Magnuson, D. & Schroeder, J. (2019) Differential privacy and Census data: implications for social and economic research, *AEA Papers and Proceedings*, 109, 403-408. DOI: 10.1257/pandp.20191107

Sansone, S., Gonzalez-Beltran, A., Rocca-Serra, P., Alter, G., Grethe, J. S., Xu, H., Fore, I. M., Lyle, J., Gururaj, A. E., Chen, X., Kim, H., Zong, N., Li, Y., Liu, R., Ozyurt, I. B., & Ohno-Machado, L. (2017) DATS, the data tag suite to enable discoverability of datasets, *Sci Data*, 4, 170059. DOI: 10.1038/sdata.2017.59

Miksa, T., Walk, P., Neish, P., Oblasser, S., Murray, H., Renner, T., … Jones, S. (2021). Application Profile for Machine-Actionable Data Management Plans. *Data Science Journal*, 20(1), 32. DOI: 10.5334/dsj-2021-032

Sax Institute (n.d.) *SURE (Secure Unified Research Environment)* https://www.saxinstitute.org.au/our-work/sure/

Shankar, K., Eschenfelder, K. R., & Downey, G. (2016) Studying the history of social science data archives as knowledge infrastructure, *Science & Technology Studies*, 29(2), 62-73. DOI: 10.23987/sts.55691

Statistics Netherlands (Centraal Bureau voor de Statistiek) (2021) μ-ARGUS v4.2, 26 August 2021. https://research.cbs.nl/casc/mu.htm

Statistics New Zealand (2020). The Five Safes framework, 30 November 2020 https://www.stats.govt.nz/integrated-data/integrated-data-infrastructure#data-safe

Studies of Childhood, Education & Youth (SOCEY) (n.d.) https://www.socey.net/

Studies of Childhood, Education & Youth (SOCEY) (n.d.) Dataverse https://dataverse.ada.edu.au/dataverse.xhtml?alias=SOCEY

Tam, S., Farley-Larmour, K. & Gare, M. (2009/10) Supporting research and protecting confidentiality. ABS microdata access: Current strategies and future directions, *Statistical Journal of the IAOS*, 26(3,4), 65–74. DOI: 10.3233/SJI-2009-0710

Templ, M., Kowarik, A. & Meindl, B. (2015) Statistical disclosure control for micro-data using the R package scdMicro, *Journal of Statistical Software*, 67(4), 1-36. DOI: 10.18637/jss.v067.i04

Trewin, D., Andersen, A., Beridze, T., Biggeri, L., Fellegi, I. & Toczynski, T. (2007). *Managing Statistical Confidentiality and Microdata Access: Principles and Guidelines of Good Practice*, UNECE/CES. https://unece.org/fileadmin/DAM/stats/publications/Managing.statistical.confidentiality.and.microdata.access.pdf

United Kingdom Data Archive (UKDA) (n.d.) *Code of Practice*, https://dam.ukdataservice.ac.uk/media/144901/sds_code_of_practice.pdf

University of Queensland (2020). *Data, materials and records management*, 4 March 2020 https://research.uq.edu.au/research-support/ethics-integrity-and-compliance/research-integrity/data-materials-and-records-management

Weaver, B. & Richardson, J. (2021). Reinventing library research support services at Griffith University, In: Fernandez-Marcial & Gonzalez-Solar (eds), *Cases on Research Support Services in Academic Libraries*, 2021, p. 267-289. DOI: 10.4018/978-1-7998-4546-1.ch012

Woolley, J. P., Kirby, E., Leslie, J., Jeanson, F., Cabili, M. N., Rushton, G., Hazard, J. G., Ladas, V., Veal, C. D., Gibson, S. J., Tassé, A., Dyke, S. O. M., Gaff, C., Thorogood, A., Knoppers, B. M., Wilbanks, J. & Brookes, A. J. (2018) Responsible sharing of biomedical data and biospecimens via the "Automated Discovery and Access Matrix (ADA-M), *npj Genomic Medicine*, 3, 17. DOI: 10.1038/s41524-081-0057-4